A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY MAGAZINE

JANUARY 2023

STEVE LOKENSGARD
PARTNER AT FAEGRE DRINKER BIDDLE & REATH IN MINNEAPOLIS, MN

LIKE SOLVING A PUZZLE (P8)

HCCA®

Compliance Risk Assessment and Management

February 22–23, 2023 | Virtual (Central European Time)

April 20-21, 2023 | Anaheim, CA ***IN-PERSON***

June 26–27, 2023 | Virtual (CT)

September 27–28, 2023 | Virtual (CT)

December 12–13, 2023 | Virtual (CT)

Get guidance and insights from experienced compliance professionals on how to conduct more effective risk assessments.

Key topics

- Risk assessment: introduction, definitions, and objectives
- Identification of compliance risks
- Assessing the severity of compliance risks
- Risk appetite and tolerance
- Effectiveness of internal controls
- Design and implementation of risk response/remediation plans
- Completing the compliance risk management cycle
- Integration with organizational risk management

Attendees can earn live Compliance Certification Board (CCB)® continuing education units (CEUs) for participating.

Register
corporatecompliance.org/cram

SCCE® Society of Corporate Compliance and Ethics

HCCA® Health Care Compliance Association

The role of compliance in workplace mental health

by Gerry Zack

For inspiration in writing this month's column, I looked no further than my own colleague, Adam Turteltaub, SCCE & HCCA's chief engagement and strategy officer, who wrote a piece for the Society of Corporate Compliance and Ethic's blog about new guidance on workplace mental health and well-being issued by the U.S. Surgeon General. I'd like to drill down on a couple of the Surgeon General's points that have relevance for compliance professionals.

The guidance describes five essential elements for workplace mental health and well-being:[1]

- Protection from harm
- Connection and community
- Work/life harmony
- Mattering at work
- Opportunity for growth

Underlying each element are several components. Like so many frameworks, successfully following this guidance requires collaboration among multiple departments, such as human resources and others. But the issue of culture comes up repeatedly throughout all five components. And culture is an area in which compliance professionals can have a direct impact.

For instance, one component mentioned under "protection from harm" in the guidance is operationalizing diversity, equity, inclusion, and accessibility norms, policies, and programs. Compliance professionals can contribute to this by making compliance training and policies more accessible for individuals with visual or hearing impairments, or by offering multiple languages. The list of diversity, equity, inclusion, and access considerations for compliance professionals in managing a compliance program is a lengthy one.

Another component—this one underlying work/life harmony—is for employers to provide more autonomy over how work is done. This scares some compliance professionals, but it shouldn't. They don't mean autonomy over whether to comply with laws, or even whether to comply with policies. But compliance professionals should always have a mindset of working with business units to develop processes that comply with laws and regulations but are also efficient. Listening to input from employees is an important consideration in developing processes and policies that are both compliant and operationally efficient.

In a related matter, one of the components under "mattering at work" is to engage workers in workplace decisions. When compliance, or business unit managers, make decisions without input from workers, resentment and dissent can easily creep in. Obviously, compliance professionals always have to keep the critical goal of complying with laws and regulations as their primary focus but helping to establish paths to compliance that engage workers and create efficiencies puts compliance in a position of creating internal value. CT

Gerry Zack
CCEP, CFE, CIA
(gerry.zack@corporatecompliance.org, twitter.com/gerry_zack, linkedin.com/in/gerryzack) is CEO of SCCE & HCCA, Eden Prairie, MN. Please feel free to contact Gerry anytime to share your thoughts: +1 612.357.1544 (Cell), +1 952.567.6215 (Direct).

Endnotes

1. Office of the U.S. Surgeon General, *The U.S. Surgeon General's Framework for Workplace Mental Health & Well-Being*, 2022, https://www.hhs.gov/sites/default/files/workplace-mental-health-well-being.pdf.

COMPLIANCE TODAY
A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

January 2023

Features

Columns

Departments

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

HCCA®
Health Care Compliance Association

888.580.8373 | hcca-info.org

Articles

Compliance Today (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6462 City West Parkway, Eden Prairie, MN 55344. Subscription is free to members (a $325 value). Periodicals postage-paid at St. Paul, MN 55112. Postmaster: Send address changes to *Compliance Today*, 6462 City West Parkway, Eden Prairie, MN 55344.

VOLUME 25, ISSUE 1

Beat the price increase: register by February 1!

27th Annual

Compliance Institute

April 23–26, 2023 • Anaheim, CA
April 24–26, 2023 • Virtual

Join your fellow healthcare professionals for the Compliance Institute, HCCA's premiere educational and networking event, offered in-person in Anaheim or as a virtual experience from the comfort of your home or office. No matter which option you choose, you'll gain connections, insights, and strategies that will help you drive success within your healthcare organization.

IN-PERSON • APRIL 23–26 • Anaheim

- 121 educational sessions
- Face-to-face interaction with session speakers, other attendees, and solution providers
- Interact with the virtual audience and view live broadcast sessions from anywhere
- 14 different topic tracks to choose from
- Up to 26.4 live CCB CEUs
- Optional Compliance Certification Board (CCB)® exams offered on the last day
- Participate in a local volunteer project
- SpeedNetworking activity (pre-registration required)
- Evening networking receptions
- 60-day access to all session recordings post conference

VIRTUAL • APRIL 24–26

- 63 live-streamed educational sessions
- 12 different topic tracks to choose from
- Up to 19.2 live CCB CEUs
- 60-day access to all session recordings post conference
- Live chat, Q&A, and polling opportunities through our robust virtual platform
- Virtual networking with both in-person and virtual attendees
- Learn more about CCB's remote proctored exam option

Sign up by February 1 to save
hcca-info.org/2023CI

HCCA
Health Care Compliance Association

HCCA association news

CI 2023: see you in Anaheim or virtually!

hcca-info.org/2023CI

Health Care Compliance Association® (HCCA®) is gearing up for the 27th Annual Compliance Institute (CI) and we hope you'll join us! Whether you attend in-person April 23–26 in Anaheim or participate virtually April 24–26, you'll learn the latest updates on real-world compliance issues, discuss emerging trends, and come away with practical applications to strengthen your compliance program.

With the evolving importance of telehealth, growing importance of and focus on mental health, and ever-changing government regulations, it's an important time to gather with experienced industry professionals to share ideas and insights, explore new strategies, get the most current information, and expand your network. Whether you join us virtually or in-person, you'll have the ability to explore a wide range of topics and home in on the issues most relevant to you.

Session tracks this year include:

- Auditing and monitoring
- Behavioral health
- Case studies
- Compliance law
- General compliance/hot topics
- How to succeed as a compliance officer
- Discussion Group (in-person only)
- Investigations
- Managed Care (in-person only)
- Physician compliance
- Post-acute care
- Privacy and security
- Risk management
- Telehealth

Pricing and registration details are available at hcca-info.org/2023CI. An early-bird registration discount applies for those who register by February 1, so be sure to beat the price increase! We look forward to having you with us at CI, whether in Anaheim or virtually.

Learn more and register
hcca-info.org/2023CI CT

Go digital and expand your healthcare compliance toolkit!

As an essential resource for healthcare compliance professionals, the *Complete Healthcare Compliance Manual* provides new and experienced practitioners with first-class guidance and insights on the fundamentals of program management.

When you opt for the digital version with an online subscription or bundle purchase, you'll receive access to additional bonus materials!

AVAILABLE IN THREE OPTIONS

One-year online subscription + Bonus resources!	**Money-saving online/print bundle + Bonus resources!**	Softcover print book

Exclusive online bonus resources include:

- Free subscription to *Healthcare Compliance Forms and Tools* (a $319 value) — This collection of sample policies, procedures, checklists, and other tools can be downloaded and easily customized for your organization. Content includes:
  - Sample board reports
  - Sample compliance risk assessment questionnaire
  - Sample compliance monitoring plan
  - List of compliance policies
  - Provider-based compliance audit checklist
  - Sample internal audit plan
  - Plus many more
- Free access to United States Code through clickable citations
- Free access to Code of Federal Regulations through clickable citations

Learn more
hcca-info.org/chcm

HCCA
Health Care Compliance Association

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.

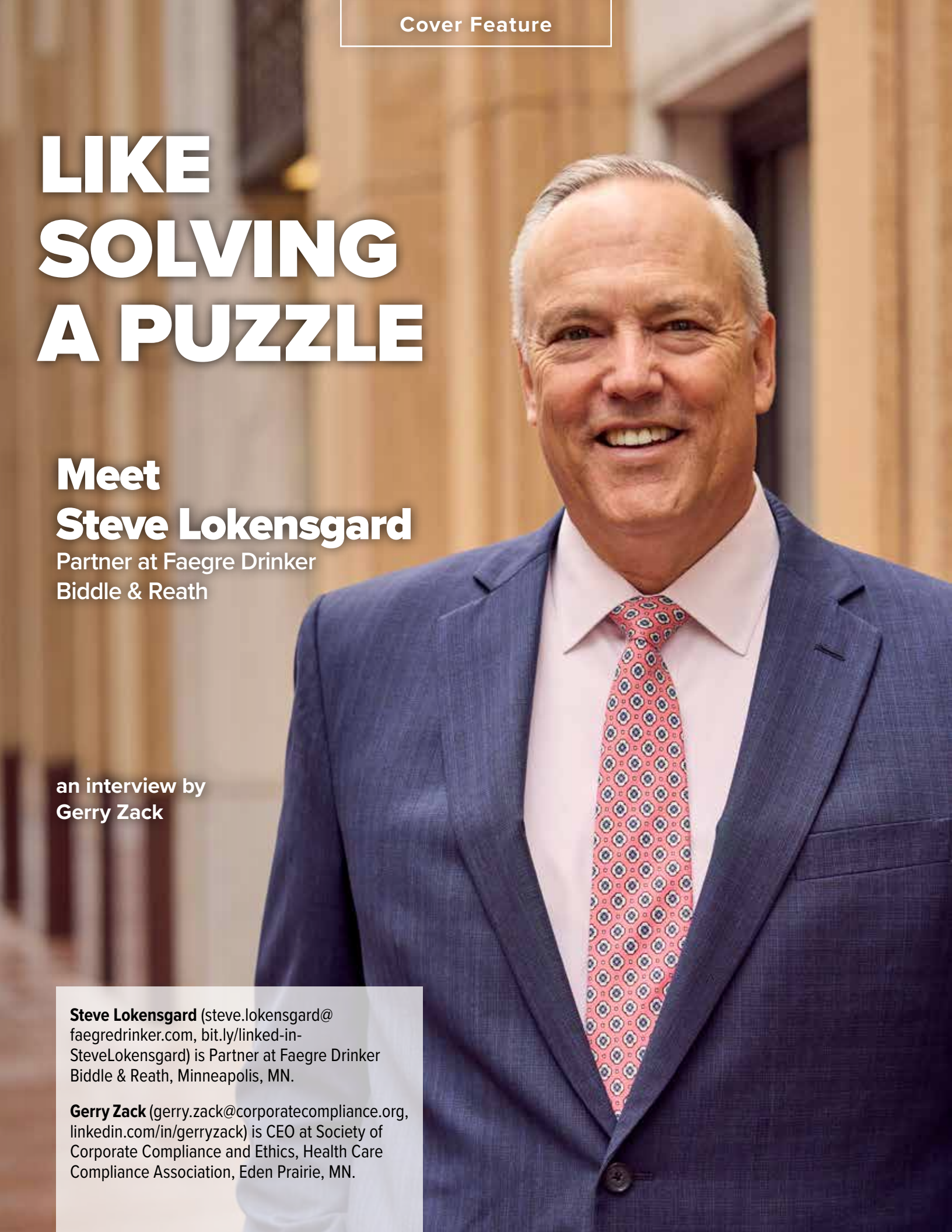
To submit your news, email
margaret.dragon@corporatecompliance.org

- **Matt Frederiksen-England**, DHA, was recently named chief compliance officer at University of Missouri Health Care.
- **Jennifer Mason**, CHC, was recently named new senior vice president and chief compliance officer at ScionHealth, Lexington, KY.
- **Michael McAuliffe**, CHC, CHPC, has been appointed compliance officer at Emerson Hospital, Concord, MA.
- **Michael A. Onusko**, CHC, has been named director of compliance, southwest region at Penn Highlands Healthcare, Monongahela, PA.
- **Kimberly Speakman** has been named chief compliance officer at American Addiction Centers, Brentwood, TN.
- **Richard Velardi** has been named director of compliance at Axsome Therapeutics Inc., New York, NY.

LIKE SOLVING A PUZZLE

Meet Steve Lokensgard

Partner at Faegre Drinker Biddle & Reath



an interview by Gerry Zack

Steve Lokensgard (steve.lokensgard@faegredrinker.com, bit.ly/linked-in-SteveLokensgard) is Partner at Faegre Drinker Biddle & Reath, Minneapolis, MN.

Gerry Zack (gerry.zack@corporatecompliance.org, linkedin.com/in/gerryzack) is CEO at Society of Corporate Compliance and Ethics, Health Care Compliance Association, Eden Prairie, MN.

GZ: You have great experience as both a compliance officer and, more recently, as outside counsel with a law firm. But your first position after law school was as a judge advocate in the U.S. Army. Tell us how you came to become a judge advocate and how that experience impacted your views on compliance.

SL: Since I was in the eighth grade, I knew I wanted to be an attorney. Maybe it was a love of history and an interest in government. At one time I was interested in politics as well, and I thought being an attorney was an essential stepping stone to understanding how the government worked. I like to tell people I grew up wanting to negotiate arms treaties with the Soviets, and I became a Medicare billing compliance attorney. Such is life!

In addition to my interest in the law, I was also interested in serving in the military. My dad was an officer in the Army Reserve. In college, I participated in ROTC [Reserve Officers' Training Corps], was commissioned as a field artillery officer, went to law school, and then became a judge advocate. I was on active duty for seven years, then in the Minnesota Army National Guard for a total of 25 years of service. Most of my time on active duty was related to military justice. I was a prosecutor, a defense counsel, and a legal adviser to the Criminal Investigation Division command.

One significant experience from my time in the Army was an understanding that the first report was almost always wrong. At least the first report usually lacked the complete picture relevant to making a decision. As much as the Army strives for clarity in communication, the "fog of war," as they say, sometimes makes it difficult to ascertain the truth as quickly as you'd like. Deliberate and careful investigations take time, and you should not rush to conclusions. Do the work, conduct a thorough investigation, and then report your findings clearly and truthfully.

Another experience had to do with the way the Army trains soldiers. They used a variety of teaching techniques to train soldiers who had different learning styles. In addition to traditional classroom training, there were many practical demonstrations and a lot of hands-on experiences. I even remember seeing books that looked like cartoon magazines used to train soldiers on how to service a vehicle. We can only hope to be as creative in training employees on essential compliance topics.

Finally, I was blessed throughout my Army career by advising leaders who wanted my advice and listened to it. Leaders play such a big role in creating a corporate culture. If you have an ethical and thoughtful leader who seeks out and takes into account advice from their legal and compliance teams, you will likely find an ethical organization that sees compliance as a core value.

GZ: From there, you went on to work as an assistant attorney general (AG) in Minnesota before then entering the field of healthcare compliance. How did you get involved in healthcare, and what are some key takeaways from your time at the AG's office?

SL: When I interviewed at the Minnesota AG's office, I was asked what I was interested in doing and I said, "Something to do with nursing facilities." The person who was interviewing me had apparently never heard that before. She burst out in laughter and had to call another deputy AG immediately and report this strange answer. For the next seven years, I litigated nursing home cost report rate appeals! I provided advice to several state-run hospitals and represented the Minnesota Department of Human Services in several Medicaid cases. I got to understand cost reporting and the economics of healthcare, but also appreciate the policy considerations underpinning a publicly funded healthcare program.

Even if you have a sympathetic regulator, it is sometimes difficult for regulators to make concessions because of the way a statute or regulation is written.

One key takeaway was that it was relatively easy to identify a noncompliant provider. With many providers who found themselves in trouble, there was frequently no intent to violate the law. But they lacked an infrastructure that would help them operate in a highly complex regulatory environment. Even if you have a sympathetic regulator, it is sometimes difficult for regulators to make concessions because of the way a statute or regulation is written. As Justice Oliver

Wendell Holmes once wrote, you must "turn square corners" when you deal with the government. I definitely grew to appreciate the value of operating an effective compliance program.

Another major takeaway is that, at least in Minnesota, there is a wealth of very knowledgeable public servants who are willing to meet with you and answer questions about complex regulations. They want the industry to succeed. Even though many of the friends I worked with have since changed jobs or retired, I still have found the staff in the agency to be very approachable, professional, and willing to help you find the right answer. You should figure out who in your company will be the contact with the agency—compliance, legal, or regulatory affairs. And in any communication with the government, you need to think strategically, but don't be afraid to reach out for help.

GZ: In moving from the AG's office—which is responsible for prosecuting individuals and organizations—to a role as associate general counsel and then chief compliance officer for a healthcare organization, there must have been some interesting challenges with such a significant shift in roles. Can you explain what it was like to experience and manage this type of change in careers?

SL: The transition from advising the Department of Human Services to advising the compliance department was not as difficult as you would think. Litigation experience was helpful in conducting internal investigations and assessing the seriousness of an issue. Experience researching and advising on billing compliance issues was similar, just viewing the world from a provider's lens rather than a regulator's lens. What was new to me were wacky Medicare compliance rules, like the "three-day payment window," the "Anti-Markup Rule," "incident-to billing," and "provider-based status." It took a while to learn about those unique Medicare billing rules, but I had good teachers!

To me, the biggest change was transferring from the law department to the chief compliance officer role. Suddenly I wasn't just providing advice (as important as that is), I was fully enmeshed in operations. You realize that the compliance issues that found their way to the legal department were really just the tip of the iceberg. Managing the compliance hotline, performing excluded provider checks, and putting together compliance education were all tasks that I hadn't been involved in as a legal adviser. I spent a lot of time identifying risks and developing mitigation strategies. The RAC [recovery audit contractor] audits were just starting when I was the compliance officer, so it wasn't hard to identify short stays as a key risk issue for all hospitals. But other than that, there were hundreds of issues identified in the OIG [Office of Inspector General] Work Plan. You appreciate the need to prioritize and mitigate risk in a variety of different ways.

GZ: Now, as a partner with a law firm, you serve many clients and work with numerous compliance programs. How have your past experiences helped, or challenged, you in this role?

SL: My legal background sometimes causes me to focus on the legal aspects of a particular issue when the real problem may be operational. In other words, the solution needs to be not only legally compliant, but also easy to implement or you are setting your organization up to fail. We should remember that the solution needs to be easy to ensure that the fix sticks.

My experience with a variety of compliance programs helps me assess the effectiveness of compliance programs of all different sizes. You develop a sense of when a company should have a standalone compliance officer, when a company should have an entire compliance department, and when a dual-hatted compliance office is appropriate. The U.S. Sentencing Guidelines note that one size does not fit all. The structure of a compliance program needs to be appropriate for that particular company.

GZ: Now that you've spent 35 years practicing law, you've probably seen and worked with compliance programs of all types and levels of maturity. What are the most common aspects of compliance programs that you find organizations asking you about, and why do you think that is?

SL: Healthcare compliance is still a relatively new profession. Compliance programs began emerging in healthcare in the 1990s and didn't really become mandatory for all providers until the Affordable Care Act in 2010. As a result, perhaps the

most frequent question I get is about the scope of a compliance program versus the scope of a law department, and how the general counsel and compliance officer should divvy up the work. Lines get blurred in smaller organizations when the sole attorney in the organization is also the compliance officer (and the risk manager). As the organization grows, it's important to clarify those lines to ensure an effective compliance program focused on mitigating compliance risks.

GZ: What is it about the current state of compliance in healthcare that has changed the most from when you started?

SL: Two developments stand out in my mind. First, 20 years ago many chief compliance officers were attorneys and former federal prosecutors. Today, many compliance officers came up through the ranks, either in compliance or other operational areas and are seen as great operational leaders within their companies rather than a former regulator. Second, compliance staff these days have taken classes on compliance programs, and many are Certified in Healthcare Compliance (CHC). I think compliance has always attracted those who are good problem-solvers, trainers, and operators. But the professionalization of the compliance staff adds a common vocabulary to the compliance department that will really help the organization succeed.

GZ: You also serve on the board of directors of a healthcare organization. With your background in law and as a compliance officer, you could be either the dream board member or a nightmare—which is it? But more seriously, how do you strike the right balance between your extensive and detailed knowledge of healthcare compliance and the need to focus on the oversight role of a board member?

SL: Luckily for St. Mary's Health Clinics, I specialize in billing compliance and the clinic doesn't bill anybody for anything! So, my legal skills are largely, shall we say, underutilized. But it is fun to sit on a board and see an organization from the board member's perspective rather than the legal or compliance perspective. Rather than running the day-to-day operations of the organization, a board member has a fiduciary duty to exercise oversight of the company's operations and ensure that the nonprofit mission is being fulfilled. It requires much more of a strategic focus than an operational or a tactical focus. I can certainly appreciate the challenge presented to board members who might not be in the healthcare field to understand the risks associated with the healthcare industry and ensure that the risks are adequately addressed by the company.

GZ: You've been a member of the Health Care Compliance Association (HCCA) for 15 years and have been active as a speaker at many HCCA events. For someone who is just getting started in their compliance careers, what advice would you have for getting involved as a speaker or author? What are the benefits of volunteering in this manner?

SL: If you think an issue is interesting, chances are many others would think it's interesting as well. Dig in. It could be an interesting issue that you just researched, or a new rule or CMS [Centers for Medicare & Medicaid Services] guidance that was just published. Dig in. Write about it or give a presentation about it. I guarantee that for every article I ever wrote and every presentation I ever gave, I learned something. It is a great exercise in professional development, and you're helping others at the same time. Also, a big benefit of speaking at a national HCCA conference is free registration and some reimbursement for travel. As more and more companies tighten their belts and don't have money to pay for an out-of-state conference, this becomes a crucial way to pay for your trip yourself and benefit from an incredible networking opportunity. The connections you make at national conferences—particularly when you're a speaker—will pay dividends the rest of your career.

The connections you make at national conferences—particularly when you're a speaker—will pay dividends the rest of your career.

GZ: For the last couple of years, you've served as an instructor for HCCA's Compliance Essentials Virtual Workshops. In addition to your deep knowledge of healthcare compliance, you clearly bring a passion for what you do to these workshops. You clearly enjoy what you do. What is it about your career that keeps that drive and enthusiasm going so strongly?

SL: First, I love teaching about the history of compliance because I think it's a really fascinating area. History has always been a big interest for me, so talking about how medicine was regulated in the late-1800s and the advent of compliance programs coming out of the "Peace Through Strength" program a hundred years later is just really fun for me. Second, regarding both the practice of law and compliance, you are presented with a wide variety of issues every day. Solving them is like solving a puzzle. It requires a little knowledge, experience, focus, and collaboration to get it done right.

GZ: But everyone needs a break occasionally. What does Steve Lokensgard do to get a breather from compliance?

SL: I think I'm a pretty classic Midwesterner. I love to grill brats and smoke ribs. I love all sports—the Minnesota Vikings, Twins, Timberwolves, and Wild. I love to go on beautiful bike rides with my wife (frequently stopping at a local tap room), play golf and cornhole, and snowmobile in the winter. I like reading historical fiction, especially if it relates to pirates. Like compliance officers, they also lived by a certain code.

GZ: Thanks so much for sharing your history and insights with us, Steve! CT

2023 Healthcare Compliance Academies

Basic – Privacy – Research

Get in-depth, classroom-style training in the essentials of managing a compliance program within a healthcare organization. Receive guidance from experienced faculty, explore a core curriculum of compliance program elements, earn Compliance Certification Board (CCB)® continuing education units (CEUs), and connect with other practitioners.

Healthcare Basic Compliance Academies

Get a better understanding of how to help your organization manage compliance risks.

Orlando, FL • Jan 23–26

Phoenix, AZ • Mar 6–9

Nashville, TN • Apr 3–6

Chicago, IL • May 8–11

New Orleans, LA • Jul 24–27

Washington, DC • Aug 21–24

Orlando, FL • Dec 11–14

...and more to come!

CHC™

Healthcare Privacy Compliance Academies

Learn how to comply with a growing body of laws and take more control over your privacy program.

Orlando, FL • Jan 23–26

Phoenix, AZ • Mar 6–9

Chicago, IL • May 8–11

Washington, DC • Aug 21–24

Orlando, FL • Dec 11–14

...and more to come!

CHPC™

Healthcare Research Compliance Academies

Discover emerging risks and solutions to increase the effectiveness of your research compliance program.

Phoenix, AZ • Mar 6–9

Orlando, FL • Dec 11–14

CHRC™

Attendees can also take an optional certification exam offered on the last day of their Academy.

CCB® COMPLIANCE CERTIFICATION BOARD

Learn more

hcca-info.org/academies

HCCA® Health Care Compliance Association

HOW COMPLIANCE CAN IMPACT ESG

by Nakis Urfi

Nakis Urfi

(nakis.urfi@babylonhealth.com, linkedin.com/in/nurfi, twitter.com/nakisurfi) is Product Compliance Officer at Babylon Health's US headquarters based in Austin, TX.

Environmental, social, and governance (ESG) programs are becoming more embedded within a company's overall strategy; compliance has an opportunity to inform and shape the development within this area.

By paying attention to ESG, one starts to notice it is hard to keep track of all the various ESG information and trends that are rapidly evolving and generating an overload of content. Spanning across various media and perspectives—the news, reports, and individual opinions—ESG content has ranged from "It will save the world" to Elon Musk calling it a scam to academic and financial institutions theorizing on the future states of ESG to anti-ESG movements evolving—and everything in between.

What is ESG?

ESG are nonfinancial factors investors use to measure investments and companies and their overall sustainability impact.

ESG's near-term goal is identifying relevant material issues important to a company's stakeholders, developing targets to positively address these issues, and sharing public reporting metrics on a company's progress toward these targets.

ESG's long-term goal is for industries to use consistent standards so rating agencies and investors can assess the value and risks of companies for investment purposes when comparing companies of interest. Currently, it is unclear whether companies will adopt the same standards for reporting, as they have options on what standards to use with so many different countries, industries, and entities involved.

Looking back at history, the first big multinational corporation was the Dutch East India Company in the 1600s. Then eventually came

Milton Friedman's concept that corporations' main purpose was to maximize revenue for shareholders. From there came the ideas of corporate social responsibility and the "triple bottom line" focusing on "people, planet, and profit."[1] Fast forward to today, industry commentators state that shareholder capitalism is moving to stakeholder capitalism. Corporations have shifted from focusing only on shareholders' interests to now focusing on the interests of all stakeholders.[2] Stakeholders include investors, members and patients, employees, clients, partners, regulators, communities, etc.

Depending on where one is on the ESG maturity curve, it is helpful to understand that one's organization has some form of ESG program and activities inflight; however, it may yet not have categorized them under "ESG." The following is a deeper dive into the various ESG categories.

Environmental

Some people confuse ESG with being strictly focused on climate change and carbon emissions. The environmental component of ESG is in high focus; however, as discussed later, only when the "S" and "G" are combined will you get a holistic view of one's organization's overall ESG standing.

Governments have committed to reducing a country's carbon emissions by a certain date, typically 2030, and reaching net-zero by 2050. The United States and European Union are pouring billions of dollars into helping reduce carbon emissions—most recently through legislation passed from the Inflation Reduction Act and REPowerEU plan.[3] Subsequently, organizations of all varieties made public commitments to do the same or similar in reducing carbon emissions. There are three primary categories for tracking carbon emissions, including Scope 1 (direct emissions), Scope 2 (indirect emissions – owned), and Scope 3 (indirect emissions – not owned).[4]

What gets measured gets managed

The U.S. Securities and Exchange Commission has proposed rule changes requiring public entities to include specific climate-related disclosures in their reporting.[5] As with any regulation, there will eventually need to be compliance adherence with this regulation. Additionally, many organizations make public their annual reduction strategy and commitments to reach their long-term carbon emission goals. This means organizations must accurately measure and manage their carbon emissions annually.

Other example categories that fall under "environmental" include air and water pollution, deforestation, waste management including packaging and electronics, raw material sourcing, toxic emissions, waste, etc.

Social

Healthcare is inherently aligned with the social pillar of ESG, as it encapsulates caring for patients as well as creating medications, devices, and vaccines that better population health, save lives, and provide high-quality and affordable care. The social components of ESG include having diversity, equity, and inclusion goals that extend to organizations developing a supplier diversity program. Additionally, it includes focusing on the safety and well-being of staff, as well as attraction and retention efforts of your workforce. Furthermore, it covers how organizations engage in responsible labor practices for their workforce.

Other areas within the social pillar consist of addressing social determinants of health for patients. Additional relevant categories include your organization's privacy and data security efforts. The scope of "social" can go beyond these categories and focus on other current social trends your organizations decide to address.

More progressive board charters are starting to include references to ESG as a part of the board's purview.

Governance

Generally, organizations already should have some governance maturity level. Typical governance components consist of board committees with oversight, diversity of the board members, compliance and ethics policies, political contributions, executive pay, internal corruption, and large-scale lawsuits. More progressive board charters are starting to include references to ESG as a part of the board's purview.

One great example of governance is in Samsung's *Electronics Sustainability Report 2021*. It included how they strengthened the

independence and authority of their compliance officer.

Samsung's compliance team—which previously reported to the corporate legal office—is now directly overseen by the CEO. One implemented standard requires a specific reason be cited for terminating a compliance officer to prevent any unfair disadvantage in personnel matters for reasons related to performing duties. Moreover, the compliance team has the authority to request resources from relevant teams—including personnel support as well as financial resources—when undergoing compliance activities. Additionally, the compliance officer has the right to attend all and call for board meetings, strengthening all authority related to board meetings.[6] As per this example, studying other organizations' ESG reports can unveil best practices across industries.

Where can compliance fit in?

Compliance can help the development and execution of an ESG program by helping structure and manage risks stemming from organizational ESG activities. Initially, an organization needs to first become educated. There needs to be buy-in across the organization to effectively implement an ESG program in a cross-functional and collaborative manner. Compliance should participate as a stakeholder for various reasons that will benefit overall ESG activities.

Increasing the effectiveness of an organization's ESG program can be achieved by maintaining an inventory of categories that qualify under ESG specific to that organization's activities. Global Reporting Initiative, Sustainability Accounting Standards Board, and Task Force on Climate-Related Financial Disclosures are international standards that can be used to capture data for tracking and reporting purposes. Compliance can help assess the process to confirm if the data—including carbon emissions data—being shared is going through some type of review or auditing process before being disclosed publicly.

Another area where compliance can execute is periodic publications, such as an annual company ESG report, which can help raise the profile of a particular organization. The quality and accuracy of the statements made in these publications need to be assessed.

Questions and areas to consider regarding where compliance can get involved with the development and execution of a company's ESG program include: (1) determining whether policies and procedures are being developed in conjunction with your organization's ESG activities; (2) assessing the level of education and reporting occurring internally in your organization; (3) tracking whether a company is meeting annual goals and commitments across a certain period (including disclosing such in annual reports); (4) reviewing responses to supplier questionnaires and request for proposals that now include ESG-related questions and deciding who will help ensure the breadth of these responses are on point; and (5) identifying emerging risks within an organization related to ESG and propose remediation activities.

Greenwashing

"Greenwashing" is an emerging risk receiving additional scrutiny. The Cambridge Dictionary defines greenwashing as making "people believe that your company is doing more to protect the environment than it really is."[7] The temptation for companies to overhype their sustainable practices and claims is present as the sustainability movement gains more traction and attention. Greenwashing can lead to reputational harm and serious violations. For example, in Volkswagen's emissions testing cheating violation, nearly 590,000 vehicles were "equipped with 'defeat devices' in the form of computer software designed to

cheat on federal emissions tests." In 2017, Volkswagen agreed to pay the US government $4.3 billion in criminal and civil penalties, and six executives faced fraud charges.[8] The scandal continues to disrupt Volkswagen's business, as subsequent litigation, scrutiny, and fines from various countries and groups have cost Volkswagen nearly $38.7 billion, with lawsuits from upset investors and customers set to drag on for years.[9]

What about nonprofit organizations?

While ESG primarily focuses on public companies, nonprofit organizations, including hospitals, are very much involved in ESG activities as well. Many nonprofit organizations have already been addressing components of ESG for a long time, including providing quality and affordable care for their communities and addressing sustainability in their practices. Nonprofit organizations have historically addressed natural disasters and methods to become more sustainable as part of environmental initiatives. Further, ESG broadens the scope of the issues to include addressing social determinants of health and health equity. An additional emerging area is an increased focus on reducing carbon emissions, including understanding carbon emissions from inside the organization's supply chain.

Investors are considering ESG an important factor in taxable debt. Organizations are now issuing ESG-related green or social bonds, and ESG disclosures in public documents are increasing.

Conclusion

Compliance professionals have an evolving role in ESG and can contribute value to being involved in ESG activities and discussions. Compliance already has a holistic view of their organization by working across all departments in their enterprise. Compliance professionals are by now used to taking on new responsibilities when emerging requirements arise. Compliance professionals bring an additional layer of ethics and integrity to the overall process, which will help build trust internally and externally with stakeholders. Given the scope of a compliance professional, they are well-suited to address working with standards, reporting requirements, regulatory requirements, and identifying and mitigating risks that are part of ESG efforts. From an activity standpoint, many transferrable experiences can be applied to developing an ESG program from a compliance program. In closing, compliance not only has a role in ESG but it is also well-suited to develop and lead overall ESG efforts at their organizations. CT

Endnotes

1. Jeroen Kraaijenbrink, "What The 3Ps Of The Triple Bottom Line Really Mean," *Forbes*, December 10, 2019, https://www.forbes.com/sites/jeroenkraaijenbrink/2019/12/10/what-the-3ps-of-the-triple-bottom-line-really-mean/?sh=53c973f95143.
2. Walter Spak and Jessica Lynd, "The Rise of Stakeholder Capitalism," White & Case, September 1, 2021, https://www.whitecase.com/insight-our-thinking/rise-stakeholder-capitalism.
3. Murray Douglas, "What will REPowerEU and the Inflation Reduction Act mean for hydrogen?" Wood Mackenzie, October 5, 2022, https://www.woodmac.com/news/opinion/what-will-repowereu-and-the-inflation-reduction-act-mean-for-hydrogen/.
4. greenly, "What are Scopes 1, 2 and 3 Emissions?" February 28, 2022, https://www.greenly.earth/blog-en/greenhouse-gas-emissions-scopes-1-2-and-3.
5. U.S. Securities and Exchange Commission, "SEC Proposes Rules to Enhance and Standardize Climate-Related Disclosures for Investors," news release, March 21, 2022, https://www.sec.gov/news/press-release/2022-46.
6. Samsung, *Samsung Electronics Sustainability Report 2021: A Journey Towards a Sustainable Future*, 8, accessed November 2, 2022, https://image-us.samsung.com/SamsungUS/home/pdf/Samsung-Electronics-Sustainability-Report-2021.pdf.
7. Cambridge Dictionary, "greenwash," *Cambridge Advanced Learner's Dictionary & Thesaurus* (Cambridge University Press), https://dictionary.cambridge.org/us/dictionary/english/greenwash.
8. U.S. Environmental Protection Agency, "Learn About Volkswagen Violations," updated September 27, 2022, https://www.epa.gov/vw/learn-about-volkswagen-violations.
9. Karen Matussek, "Ex-VW Manager Released Early From Diesel-Rigging Prison Term," *Bloomberg*, January 20, 2021, https://www.bloomberg.com/news/articles/2021-01-20/ex-vw-manager-schmidt-gets-early-release-from-diesel-prison-term?leadSource=uverify%20wall.

Takeaways

- Environmental, social, and governance (ESG) are nonfinancial factors investors use to measure investments and companies and their overall sustainability impact.
- Organizations are already engaging in many ESG activities, and ESG brings a new lens and framework broadly to these activities.
- Stakeholder expectations and upcoming regulations are driving the movement in the ESG industry.
- There are similarities between running ESG efforts and operating a compliance program.
- Compliance professionals bring great skill sets and capabilities that can lead or help manage ESG activities.

HCCA® webinars

Want to stay up to date on the latest in healthcare compliance?

Explore topics like regulatory updates, data privacy, managed care, telehealth, and much more from the comfort of your home or office with HCCA webinars—now more affordable than ever!

HCCA offers a robust schedule of interactive healthcare compliance webinars each year. With a single registration,* your entire team can participate in these convenient and insightful 90-minute sessions.

**All participants must be in the same physical location.*

Earn more CEUs for less

Get the opportunity to earn up to a maximum of 1.5 Compliance Certification Board (CCB)® continuing education units (CEUs) per webinar—total CEUs may be subject to change due to length of presentation.

HCCA members receive discounted registration on all webinars!

Members: $49
Non-Members: $99

See what's coming up
hcca-info.org/webinars

HCCA
Health Care Compliance Association

Improve the compliance officer's relationships through the compliance risk assessment

by Catherine Boerner

Risk assessment can strengthen the compliance officer's relationship with operational directors and managers. This process can build trust in a nonconfrontational, proactive, safe environment. This is a good process for the compliance officer to communicate—in person and during interviews—that compliance is here to partner with operations to assist in improving compliance. This is not a "gotcha" exercise or even an audit. This is an opportunity for managers and directors to communicate improvements to controls that would assist them, including additional education if needed and/or clearer policies and procedures. This is also a chance for compliance officers to communicate about the hotline if directors and managers feel the need to be anonymous after the meeting with any specific operational concerns that compromise compliance with laws and regulations.

The culture of "we are all in this together" and where everyone wants to do the right thing is important to keep in the forefront. Could there be a grey area? Yes, but let's all be comfortable with what the grey areas are and get proper legal advice, as needed, to ensure we are doing the best we can to comply with the laws and regulations. Everyone should be able to sleep at night.

The tone at the top—by the CEO and CFO—can really drive the compliance risk assessment and use it as an opportunity to communicate the need and desire for transparency for all those interviewed and involved. It is beneficial for the compliance officer to be present in the interviews even if a third party is performing the compliance risk assessment. This will help build those relationships. Sometimes the involvement of applicable vendors is also helpful in understanding everyone's roles, as it pertains to maintaining controls to mitigate risk. This is especially vital if positions are outsourced.

At the end of the day, this exercise, if done right, can truly improve the compliance officer's exposure and relationships by putting people at ease. The process can help gather information and provide valuable insight into what is working well and where the opportunities are. It can also proactively seek out discussions regarding potential risks and offer a collaborative tone to make things better. CT

Catherine Boerner
JD, CHC
(cboerner@boernerconsultingllc.com; linkedin.com/in/catherineboerner) is President of Boerner Consulting LLC, New Berlin, WI.

HCCA SALARY SURVEY REVEALS A BRIGHT COMPENSATION PICTURE

by Adam Turteltaub

Adam Turteltaub
(adam.turteltaub@corporatecompliance.org, linkedin.com/in/adamturteltaub) is Chief Engagement & Strategy Officer, SCCE & HCCA, Eden Prairie, MN.

The Health Care Compliance Association (HCCA) first surveyed compensation for healthcare compliance professionals back in 2013. The survey was last conducted in 2019, and with the pandemic-related changes to the job market, the association was eager to provide updated information for the compliance profession.

In June 2022, an email invitation was sent out to approximately 50,000 individuals on the association's mailing list requesting their participation. The responses were tabulated by an external research company to ensure both accuracy and confidentiality of the data.

A copy of the report can be found on the HCCA website.[1] Members of the HCCA can also access an interactive version in which they can run custom data queries.

Findings

Compensation has increased across the board for compliance professionals at all levels. Chief compliance officers (CCOs) responsible for 76% or more of their organization's legal risk saw an average income of $179,281, up 16% from 2019 (see Figure 1).

Looking at staff, compensation for directors averaged $142,946, an increase of 10%. Managers were at $109,791, up 13%, and the assistant/specialist levels saw an average salary of $81,078, up 8% (see Figure 2).

Compensation levels did vary considerably, though, based on where an individual works—in terms of geography and type of corporation. CCOs in the West South-Central region, for example, saw average compensation of $193,672, while those in the Mid-Atlantic region saw just $154,145.

Of even greater difference was compensation based on whether

Figure 1: Average total compensation by percentage of company's legal and regulatory risk areas CCOs involved in

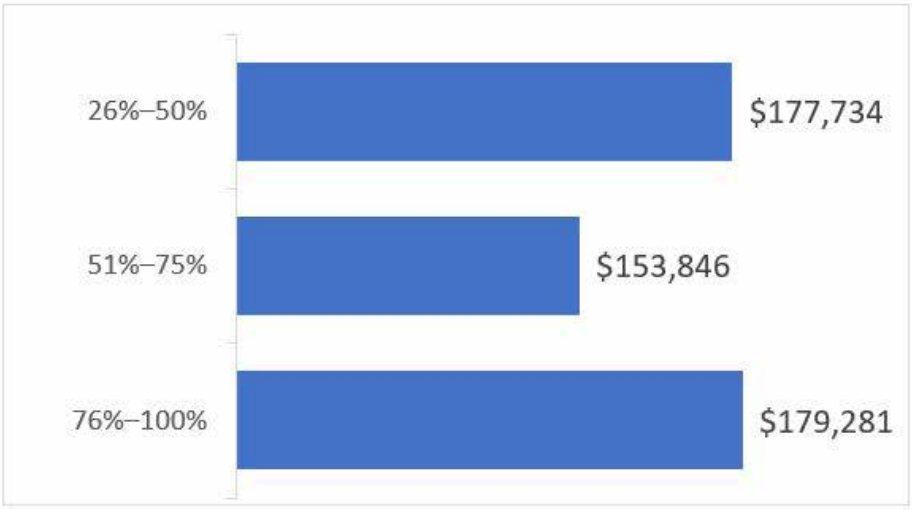


Figure 2: Average total compensation by title/level

the organization was for-profit or not. CCOs at publicly traded organizations enjoyed average total compensation of $260,871 compared to just $161,016 at nonprofits and $148,443 at governmental institutions (see Figure 3 on page 22).

At the staff level, the differences were also stark, with a manager at a publicly traded organization earning an average of $122,850 compared to $111,721 at a nonprofit and just $101,900 at an academic institution

Certification correlated strongly with higher compensation. Individuals possessing a Compliance Certification Board designation earned far more than those who did not, and individuals who had achieved Certified in Healthcare Research Compliance (CHRC) generally earned the most. (see Table 1 on page 22).

Also of note: how commonly held the certifications were, with 60% of CCOs holding the Certified in Healthcare Compliance (CHC) designation, 62% of directors, and 53% of managers.

To see more of the data be sure to visit the HCCA website: *www.hcca-info.org/publications/surveys/2022-hcca-salary-survey*.

Endnotes

1. Health Care Compliance Association, "2022 HCCA Salary Survey," October 17, 2022, https://www.hcca-info.org/publications/surveys/2022-hcca-salary-survey.

Figure 3: Average total compensation by type of organization

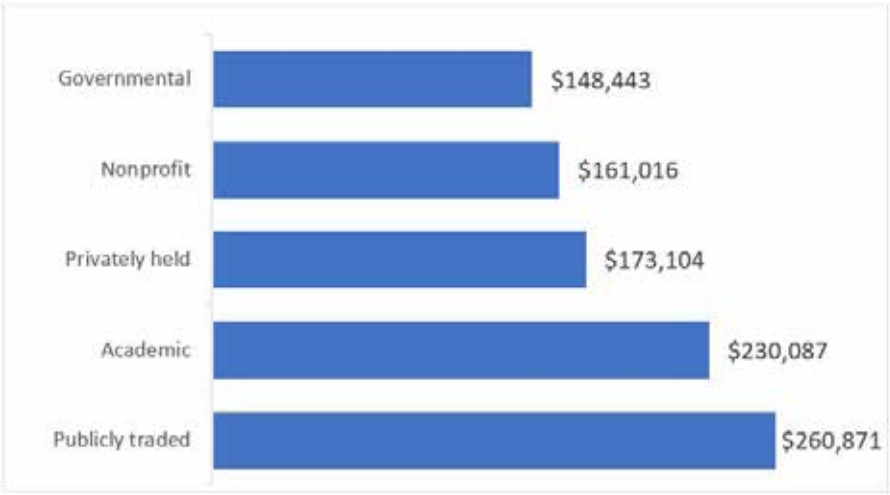


Table 1

Certification	CCO	Director	Manager	Asst/Specialist
CHRC	$246,738	$165,000	$129,950	$71,619
CCEP (Certified Compliance & Ethics Professional)	$207,323	$160,389	***	***
CHPC (Certified in Healthcare Privacy Compliance)	$202,467	$149,166	$113,409	$92,377
CHC	$186,311	$148,286	$118,875	$88,149
None	$130,152	$121,685	$96,657	$74,003

***Insufficient data

Takeaways

- Compensation has generally increased.
- Certification correlates with significantly higher salaries.
- As would be expected, larger organizations generally pay higher than smaller ones.
- Public companies typically offer the highest compensation.
- There are substantial regional variations in compensation.

OIG updates CIAs, and compliance officers should take notice

by Betsy Wade

U.S. Department of Health & Human Services, Office of Inspector General (OIG) announced several changes to its standard Corporate Integrity Agreement (CIA) that will not only impact those entering CIAs but should cause all compliance officers to consider changes to their compliance programs.[1]

Announced September 29, 2022, at the American Health Law Association's *Fraud and Compliance Forum* 2022 in Baltimore, Maryland, the changes include:

- Compliance officer's responsibilities
- Compliance committee's role and responsibilities
- Risk assessment
- Creation of a transition plan

Compliance officer responsibilities have been limited in new CIAs. CIAs previously stated that any noncompliance job responsibilities of the compliance officer "shall be limited and shall not interfere or conflict with the Compliance Officer's ability to perform." An example of a CIA with the updated requirements is between OIG and Biotronik Inc.: "The Compliance Officer shall not have any noncompliance job responsibilities that, in OIG's discretion, may interfere or conflict with the Compliance Officer's ability to perform the duties outlined in this CIA."[2] The change was made to address "job creep" related to operational responsibilities OIG has seen assigned to compliance officers over the last several years impacting their independence.

The compliance committee's role has expanded in new CIAs and now includes:

- Implementation and oversight of the risk assessment
- Annual policy and procedure review
- Annual compliance training review
- Development and implementation of the transition plan, which was described as a three- to five-year strategic plan

The OIG noted the compliance committee's engagement should be demonstrated by attendance, questions, idea contribution, and being a compliance advocate.

Risk assessments were first included in CIAs several years ago. The CIA language has been updated to reflect the compliance committee oversight responsibilities stating that the risk assessment shall be conducted annually and require:

1. Identification and prioritization of risks
2. Development of work plans or internal audit plans related to the identified risk areas
3. Implementation of the work plans and internal audit plans
4. Development of corrective action plans in response to the results of any internal audits performed
5. Tracking the implementation of the work plans and any corrective action plans and assessing their effectiveness

As a result of the new CIA requirements, organizations should:

- Evaluate compliance officer responsibilities for potential conflicts
- Revise the compliance committee charter to include new responsibilities
- Develop a compliance department strategic plan
- Educate the compliance committee and board about the latest updates

Betsy Wade
MPH, CHC, CNA
(bwade@signaturehealthcarellc.com; bit.ly/linkedin-BetsyWade) is Chief Compliance and Ethics Officer at Signature Healthcare, Louisville, KY.

Endnotes

1. Laura Ellis, Mary Findley, and Al Shay, "CIA Changes on The Horizon: What They Are and What They May Mean for You," Fraud and Compliance Forum, American Health Law Association, September 29, 2022.
2. Corporate Integrity Agreement between U.S. Department of Health & Human Services, Office of Inspector General and Biotronik, Inc., August 26, 2022, https://oig.hhs.gov/fraud/cia/agreements/Biotronik_Inc_08262022.pdf.

IDENTIFYING AND MANAGING RISKS WITH THIRD-PARTY RELATIONSHIPS

by Lisa Taylor, Amy Smith, and Kasie Ray

Lisa Taylor *(lisa.taylor@uchealth.com; bit.ly/linked-in-LisaTaylor) is Vice President & Chief Compliance Officer at UC Health, Cincinnati, OH.*

Amy Smith *(amy.smith3@uchealth.com; bit.ly/linked-in-AmyGreeneSmith) is Assistant Compliance Officer at UC Health, Cincinnati, OH.*

Kasie Ray *(kasie.ray@ankura.com) is Director at Ankura Consulting Group, Nashville, TN.*

While most organizations have a central mission and scope of services, it is not uncommon for various organizational departments to view third-party relationships and risks differently. For example, a clinical business unit may decide to contract with a vendor to provide widgets. However, that business unit does not know that the contracting vendor is about to be involved in a large-scale Anti-Kickback Statute (AKS) investigation. While there are no crystal balls to predict which third parties can create large-scale risks for an organization, it is reasonable to see that there could be compliance implications in each arrangement. One of the worst things a compliance officer or department can do is take a completely hands-off approach to third-party arrangements. Compliance leaders should establish strong working relationships with senior leadership and operational leaders. This will better enable compliance professionals to explain the risks that third parties present, generate support for the development and implementation of a compliance program, and, when needed, provide the organization with a rationale for the spending of corporate dollars to manage the program to address risks.

Third-party relationships cannot be managed without first understanding the regulations and compliance risks associated with these arrangements. These risks directly impact many of the daily legal and regulatory requirements compliance professionals encounter. It is important to understand how each of the following laws and regulations affects third-party relationships.

Federal Exclusion Statute

The Federal Exclusion Statute prohibits entities that participate in federal healthcare programs from entering or maintaining certain relationships with individuals or entities that have been excluded from participation in federal healthcare programs.[1] The U.S. Department of Health & Human Services (HHS), Office of Inspector General (OIG) has issued a special advisory bulletin emphasizing the importance of exclusion checking.[2]

Civil Monetary Penalties Law

The Civil Monetary Penalties Law (CMPL) authorizes HHS and OIG to impose civil monetary penalties, assessments, and program exclusions against any person that submits false or fraudulent or certain other types of improper claims for Medicare or Medicaid payment.[3]

AKS

Under the federal AKS, no individual or entity may offer, pay, solicit, or receive anything of value

(in cash or in-kind) directly or indirectly for federal healthcare program business referrals.[4] This prohibition is broad and covers all situations where something of value is provided free or at a discount to any potential referral source.

Physician Self-Referral Law

"The Physician Self-Referral Law, commonly referred to as the Stark law, prohibits physicians from referring patients to receive 'designated health services' [as defined in Stark] payable by Medicare or Medicaid from entities with which the physician or an immediate family member has a financial relationship, unless an exception applies."[5]

HIPAA Privacy and Security

Organizations must consider the HIPAA regulations when providing protected health information (PHI) to third-party organizations that are considered business associates (BAs) for services. Organizations must have a contract or business associate agreement (BAA) with the third party. The Privacy Rule requires, at a minimum, the agreement:

- "Describe the permitted and required uses and of protected health information by the business associate;
- "Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
- "Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract."[6]

False Claims Act

The False Claims Act (FCA) prohibits organizations from submitting claims to Medicare or Medicaid that are known (or should be known) to be false or fraudulent.[7] False claims carry hefty civil penalties of up to three times the program's loss plus an additional $11,000 per claim. In addition to the civil penalties, FCA violations can carry criminal penalties, including fines and prison time. The risks and liability associated with the FCA apply to the organization, whether they are submitting directly or if a third-party vendor they have contracted with is submitting the claims on the company's behalf. The FCA does not require proof that an organization knew the claims submitted were false. It considers if the organization *should* have known and if they acted with reckless disregard for the information or deliberate ignorance.

Physician Payments Sunshine Act

The Physician Payments Sunshine Act (also referred to as the Open Payments Program) requires drug and medical device companies to report payments and items given to teaching hospitals, physicians, and certain other clinicians.[8] Manufacturers may report and attribute payments to a specific clinician or teaching hospital. The Center for Medicare & Medicaid Services publishes this information on the Open Payments website for the public to see details about the financial interactions between drug and medical device companies, healthcare entities, and clinicians.[9] Reviewing this data can be cumbersome. However, the data can provide insights into which contractors have provided items of value that may indicate risk or concern (although not necessarily).

Not having a clear understanding of the vendors with which an organization is engaged can create a blind spot to potential risk areas.

Challenges to managing third-party relationships

While many compliance professionals are adept at handling risks within their own organizations, creating and implementing the controls necessary to manage risks created by other organizations can take much more effort. Some common gaps to consider in a third-party management process:

- **There is no comprehensive third-party/vendor list.** Not having a clear understanding of the vendors with which an organization is engaged can create a blind spot to potential risk areas. This list should include the legal name of the company, tax identification number, corporate address, an overview of the type of services the third party provides, where it provides those goods or services if its business is in the US or extends to other countries, and potential conflicts of interest.

- **A contract management system may not include third-party agreements.** Without a functioning, well-maintained contract management system, a compliance professional is unlikely to be aware of all the details required to manage the risks associated with these agreements.
- **Information and data are not being collected or utilized.** Without identifying what data sources are available and how this data can be used to successfully audit and monitor activities involving vendors, organizations cannot maintain a clear picture of how these services are working or adequately manage the risks.
- **Inadequate policies and procedures related to third-party relationships.** Policies and procedures should provide an overview of managing and interacting with the third party. For example, there should be written standards documenting the vendor onboarding requirements, vendor background checks, adherence to the code of conduct, and how to determine and manage any physical access by the vendor.
- **No buy-in from senior leaders.** Company and operational leadership may not be fully aware of the risks associated with third parties. Compliance professionals may face some resistance to oversight and review in some of the areas that utilize vendors the most. A third-party relationship management process will also have costs associated with it that will require senior management to invest in it.

Implementing effective solutions to third-party compliance management

Several steps can help effectively manage third-party arrangements from a compliance perspective.

Step 1: The selection process

Create a request for information (RFI) or request for proposals (RFP) process. Compliance professionals can help implement an RFI or RFP for prospective third parties. This allows the organization to thoughtfully document the requirements it needs in a third-party vendor, ensure the qualifications are documented, document the business rationale and intent for engaging the third party, and outline the parameters of working with the organization (i.e., the rules and regulations the third party would be expected to follow and adhere to).

- Once an RFI/RFP is sent to a variety of possible third parties, those entities wishing to do business will submit responses. This process gives the requesting organization the opportunity to review responses to ensure a fair market value (FMV) price is set for the service or product that will be purchased and that the scope or product is appropriate.
- The RFI/RFP is also the opportunity to outline some, if not all, of what the organization's contract terms will be. Contract terms should include all items that are expected of the third-party. Some terms are apparent, such as privacy and security considerations (if involving PHI), AKS and Stark risks, ensuring FMV, and outlining expectations of products or services. Some terms are less obvious, such as auditing and monitoring parameters, notification when there is an issue (e.g., breach, recall, etc.), and some of the expectations (with time frames) of the third party in all actions and when the party is on-site (if applicable).

Organizational due diligence. Many departments may need to be involved with the third-party evaluation and selection process, such as operations, legal, compliance, IT, supply chain, and human resources, among others. Organizations should have a written due diligence process. Some items to consider stem from the Department of Justice (DOJ) guidance. DOJ states that organizations should have a business rationale for utilizing third-party vendors. DOJ further asserts that organizations should have a detailed contract, ensure the contracted third party is performing the work, and that the compensation is commensurate with the work being performed in the geographic location and industry.[10] Prior to contracting, an initial exclusion check should be run against the organization per the Federal Exclusion Statute. Certain items or services may require a more thorough due diligence review because they have higher risks for the organization. For example, the highest diligence must be utilized with coding contractors, billing services, and those with access to sensitive PHI.

Step 2: Onboarding the third party and educating leadership

Compliance training and reporting. It is a best practice that all contracted third parties are provided with compliance training, the code of conduct, and appropriate policies and procedures. OIG guidance

states an organization should have an established policy outlining the compliance obligations of vendors and other third parties (including adherence to the standards of conduct).[11] Training is essential for third parties to understand their responsibilities and know how to contact compliance or report a concern. Organizations can address compliance training in various ways (e.g., online training, third-party/vendor management systems, or even via mail). Ideally, compliance training and the code of conduct should be provided before the third party is onsite or has access to any systems. If a contractor offers to use its compliance training content in place of the organization's training, it is best to request a copy of the contractor's training prior to agreeing to this option.

Conflicts of interest (COI)/gifts and entertainment by third parties. Many compliance programs likely have existing policies for COI and gifts. As a best practice, COI disclosures should be completed and reviewed on at least an annual basis. Annual training should also include content on COI and gift policies, so staff is aware of the parameters and reporting requirements. COI relationships and gifts from contractors can raise various issues, including, but not limited to, AKS and Stark risks.

Annual compliance certifications by third parties. Choosing to work with organizations that are committed to compliance is crucial when entering into third-party agreements. Organizations could consider developing an annual certification whereby the third party certifies that they have a compliance program, compliance policies, appropriate education, training, etc. This certification could be managed by procurement/vendor management.

Ensure inclusion of third-party risk in risk assessment and compliance committee discussion. An organization's compliance committee can be a great place to integrate third-party management into the overall compliance program. For example, leaders that oversee third parties in the organization can be invited to attend and report on third-party compliance matters at compliance committee meetings. This provides a forum for organizational leaders to become educated on the applicable risks and potential gaps. Additionally, third-party risk should be included in the compliance risk assessment, which is often conducted in collaboration with the compliance committee.[12]

Step 3: Managing third-party arrangements

Auditing third parties based on assessed risk or reports to compliance. As previously mentioned, auditing terms can be included in third-party contracts. A compliance program will obviously not be able to audit every third-party agreement or relationship; however, the program can focus on audits stemming from the organization's compliance risk assessment and when third-party-related reports of concerns come to the compliance department. These audits can include reviewing the third party's contract terms, books and records of the third party, commercial reasonableness of the relationship, use and disclosure of PHI, and other items depending on identified risk.

Monthly exclusion screening. Per OIG guidance, organizations should have an established policy prohibiting third parties excluded from contracting with or working in the organization.[13] There should be monthly monitoring of sanction lists and corrective action for any identified excluded third parties.

An organization's compliance committee can be a great place to integrate third-party management into the overall compliance program.

An organization could be subject to CMP liability if an excluded person or entity participates in furnishing items or services that are payable by a federal healthcare program. The risk of potential CMP liability is greatest for those who provide items or services integral to the provision of patient care because it is more likely that such items or services are payable by federal healthcare programs. In its Special Advisory Bulletin, "OIG recommends that providers screen nurses provided by staffing agencies, physician groups that contract with hospitals to provide emergency room coverage, and billing or coding contractors."[14] It is important to note that this CMP liability does not just apply to direct patient care roles or items or services furnished at the medical direction of an excluded person. CMP liability

could result even if the excluded person provides administrative and management services or volunteer services. Organizational buy-in and collaboration are essential if the exclusion screening process is to succeed. Compliance may need to partner with various internal departments to assist with exclusion screenings. Human resources, credentialing services, the medical staff office, supply chain, accounts payable, and student and volunteer services are a few departments that may be integral to the process.

Step 4: Ending the relationship

Terminating relationships and access to systems. Organizations should terminate contracts if third parties or their representatives fail to comply with policies or the code of conduct. It is essential to have a process to require and confirm that all business information (including any PHI) is returned or destroyed by the third party. Additionally, any access to organizational systems should be terminated as well (e.g., third-party management systems, electronic medical record systems, billing systems, etc.). All physical access to sites, buildings, and parking garages should also be disabled.

Conclusion

While it may seem like a somewhat daunting feat, compliance professionals can help educate their organizations about third-party risks and help foster and champion a third-party focus within the compliance program. With proper understanding, processes, buy-in, and monitoring, third-party agreements that provide value to your organization's operations can also be carried out in a compliant way to decrease risk to the organization. CT

**The views expressed herein are those of the author(s) and not necessarily those of Ankura Consulting Group LLC, its management, its subsidiaries, its affiliates, or its other professionals. Ankura is not a law firm and cannot provide legal advice.*

Endnotes

1. 42 U.S.C. § 1320a-7.
2. U.S. Department of Health & Human Services, Office of Inspector General, *Updated Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs*, May 8, 2013, https://oig.hhs.gov/exclusions/files/sab-05092013.pdf.
3. 42 U.S.C. § 1320a-7a.
4. 42 U.S.C. § 1320a-7b(b).
5. U.S. Department of Health & Human Services, Office of the Inspector General, "Fraud & Abuse Laws: Physician Self-Referral Law [42 U.S.C. § 1395nn]," accessed November 3, 2022, https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/#:~:text=The%20Physician%20Self%2DReferral%20Law%2C%20commonly%20referred%20to%20as%20the,relationship%2C%20unless%20an%20exception%20applies.
6. "Business Associates [*45 CFR 164.502(e), 164.504(e), 164.532 (d) and (e)*]," OCR HIPAA Privacy, revised April 3, 2003, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf.
7. 31 U.S.C. § 3729.
8. 42 U.S.C. § 1320a-7h.
9. CMS.gov, "Open Payments: What is the Open Payments Program?" last modified October 6, 2022, https://www.cms.gov/OpenPayments.
10. U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs," updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.
11. HCCA–OIG Compliance Effectiveness Roundtable, *Measuring Compliance Program Effectiveness: A Resource Guide*, March 27, 2017, https://oig.hhs.gov/documents/toolkits/928/HCCA-OIG-Resource-Guide.pdf.
12. U.S. Department of Justice Criminal Division "Evaluation of Corporate Compliance Programs."
13. HCCA–OIG Compliance Effectiveness Roundtable, *Measuring Compliance Program Effectiveness*.
14. U.S. Department of Health & Human Services, Office of Inspector General, *Updated Special Advisory Bulletin*.

Takeaways

- The federal government has emphasized the importance of and increased its scrutiny of third-party management practices within organizations.
- There are various compliance risks when engaging third-party contractors. Ultimately, the risk lies with the contracting entity (not the third-party contractor).
- Buy-in and a commitment to compliance throughout organizational leadership and departments are essential to effectively manage risks with third-party contractors.
- Organizations should have a formal due diligence process to evaluate potential third-party contractors and related risks. Ongoing audits, monitoring plans, risk assessments, and compliance training can be practical tools to mitigate and address risks.
- When terminating third-party contractor agreements, ensure there is a process to confirm that all business information (including protected health information) is returned or destroyed and that all access the third-party contractor had to physical sites or online sites/systems is also ceased.

The importance of training for compliance professionals

by Donnetta Horseman

Compliance professionals are charged with training the workforce. To be effective, they must stay abreast of various regulatory areas, which can be very challenging. Here are some education and training tips for the compliance officer.

Subscribe to government and regulatory agency listservs

The U.S. Department of Health & Human Services, Office of Inspector General, and Office for Civil Rights offer listservs to inform you about important news from these agencies. Most Medicare administrative contractors and state health agencies also offer listservs or periodic newsletters to provide significant updates.

Attend webinars and conferences

All compliance professionals should dedicate time to professional development. It is often the last thing we think about and the first thing to be sacrificed when there are other pressing demands. We are doing ourselves a disservice by not staying current. Hundreds of organizations provide regular webinars—some at no cost—and key healthcare compliance conferences are designed to offer professional development. For instance, the annual Compliance & Ethics Institute, Healthcare Enforcement Conference, and other subject-matter conferences offered by the Health Care Compliance Association & Society of Corporate Compliance and Ethics. These are prime opportunities to hear from top regulators, enforcers, and other subject matter experts.

Take advantage of expert summaries

Many law firms have dedicated healthcare law sections that provide expert summaries of new or changing regulations. You do not have to be a customer to subscribe to receive these updates. They typically offer an executive summary, along with a more in-depth look at the topic, law, or regulatory change. These are also excellent resources to share with senior leadership and the board.

Network with peers

One of the biggest benefits of attending conferences is networking with peers. There is no better form of education and training for compliance officers than learning from others in the same field. Connecting with peers not only gives you a laundry list of contacts to call when you need to phone a friend for help, but it can also broaden your exposure to compliance subject matter areas outside your personal experience. Additionally, many professional organizations have private listservs and websites that give you access to hundreds, if not thousands, of other compliance professionals.

Staying well-informed of new laws and regulatory changes is critical to being an effective compliance professional. CT

Donnetta Horseman

(donnetta.horseman@moffitt.org; bit.ly/in-DonnettaHorseman) is Chief Compliance Officer at H. Lee Moffitt Cancer Center and Research Institute, Tampa, FL.

THE IMPORTANCE OF A ROBUST THIRD-PARTY COMPLIANCE PROGRAM

by Amy B. Boring and Stephen P. Cummings

Amy B. Boring
(aboring@kslaw.com) is Partner at King & Spalding LLP, Atlanta, GA.

Stephen P. Cummings
(scummings@kslaw.com) is Counsel at King & Spalding LLP, Atlanta, GA.

Each year, companies devote vast financial, technical, and staffing resources to implement and maintain effective corporate compliance programs. Generally, an effective compliance program has seven essential elements, including standards, policies, and procedures; compliance program administration; screening and evaluation of employees, vendors, and other agents; communication, education, and training; monitoring, auditing, and reporting; discipline for noncompliance; and investigations and remedial measures.[1] For example, American hospitals spend almost $39 billion annually on regulatory compliance activities.[2] Understandably, most compliance work is focused on a company's internal business operations, including ensuring that the company's employees are familiar with applicable policies and procedures; receive regular training; know how to report compliance concerns; and that there is a process in place to investigate and resolve compliance concerns and complaints.

But increasingly, companies are turning their compliance focus to include a more robust examination of a company's third-party vendor relationships because there is growing recognition that third-party vendors can introduce significant compliance risk into a company's business environment. This renewed focus is reasonable considering the increased interest regulators are showing concerning third-party relationships. Indeed, the U.S. Department of Justice has issued explicit guidance that called out third-party management as an essential feature of a well-designed corporate compliance program.[3] Therefore, it is important that companies take steps to ensure that their existing compliance programs comport with the current guidance for what constitutes an effective third-party compliance program.

The third-party vendor relationship life cycle

Without question, third-party vendors are vital in many companies' business operations, but using third parties also creates substantial regulatory and enforcement risks. As such, it is imperative that a company compliance program includes an effective process to manage and mitigate potential third-party vendor risks.

An essential first step in the creation and implementation of a third-party compliance program is identifying all third parties

that need to be included in the compliance process, which consists of all third parties that touch any aspect of a company's business environment—both upstream and downstream with respect to sales, products, personnel, and services. The next step in the process is the development of a program that addresses all facets of a third-party vendor relationship, which includes:

- Business rationale or justification
- Risk-based vendor due diligence
- Contracting to limit the risk of vendor noncompliance
- Onboarding
- Monitoring and auditing of vendor compliance
- Concluding the relationship

Business justification

The initial phase of the third-party vendor relationship life cycle is to have a defined process for determining when there is an actual business need to engage a third-party vendor. The process should, at a minimum, include the purpose of the vendor, who requested the vendor, who approved the hiring of a vendor, and the creation of a file where the information pertaining to the other vendor life cycles is collected and maintained.

The importance of knowing whom you are doing business with

The second phase of the life cycle ensures the company knows who it proposes to do business with by conducting risk-based diligence. A risk-based approach to diligence is crucial because not all vendors require the same amount of due diligence. In implementing a risk-based approach, a company should have a defined process to evaluate what level of diligence is required for each vendor type.

For example, if a hospital hires a vendor to supply paper for copy machines, this business activity appears to involve minimal compliance risks, so a lower level of diligence is likely appropriate. In contrast, if a hospital engages a vendor to manage its electronic health records, the potential compliance risks associated with this business activity are substantial, so a much more vigorous diligence process is required.

One potential challenge in knowing your business partner is that if potential red flags are identified during the diligence process, these flags must be resolved and documented to avoid a situation where a regulator second-guesses the decision to engage a particular vendor. Another challenge is maintaining the historical diligence file so that a company can demonstrate the reasonableness of its diligence process after the fact. There are also circumstances where postcontractual diligence may be appropriate, especially when a vendor has access to highly sensitive information or in the cases of long-term contracts where it may be years before a vendor undergoes another diligence review.

Contracting to limit risk

The third phase in the life cycle is using contracts with regulatory compliance standards to mitigate potential third-party vendor risks. Indeed, depending on the nature of the business activity, it may be advisable to adopt specific regulations or legal standards in the contract. For instance, in the hospital example relating to electronic healthcare records, it may be advisable to have contractual provisions that explicitly address compliance with HIPAA, confidentiality, privacy, and cybersecurity. Another way that a company can seek to limit its risk is by including contractual provisions that require a third-party vendor to use written policies and procedures, conduct regular compliance training, maintain a compliance program, and report compliance violations.

Depending on the nature of the business activity, it may be advisable to adopt specific regulations or legal standards in the contract.

Suitable onboarding

The fourth phase is the use of an onboarding process that clearly spells out compliance expectations and requirements. The amount of onboarding will vary depending on the third party's business activity; however, it can include acknowledgment of receipt and review of applicable policies and procedures, initial and annual training requirements, and familiarization with compliance reporting requirements. The last point is particularly significant because it is not uncommon for third-party vendors to be unfamiliar with how to report compliance concerns in a timely manner and/or to the appropriate persons.

Monitoring and enforcement

The fifth phase—and the single best way to mitigate the risk associated

with third-party vendors—is to adopt a comprehensive monitoring process to ensure that the vendors comply with all applicable contractual provisions and legal obligations. But monitoring by itself is not enough. A company must also have a process for reviewing and resolving any potential red flags identified during the monitoring process. This includes making sure the investigation is documented, including documentation for why an event is not a compliance risk. Moreover, compliance violations must be remediated, and where appropriate corrective action should be taken and documented. Additionally, if there is a pattern or practice of violations, the company should take steps to address any systemic deficiencies, which may include additional training, modifications of policies and procedures, or additional monitoring/auditing.

Concluding the relationship

Once a third-party vendor relationship ends, this should be noted, and the appropriate records retention policy should maintain all relevant files. In addition, there should be a process to ensure that the vendor no longer has access to confidential business information and that it returns all company property and information. For example, when a vendor's contract expires, access to the company's business offices and network should be terminated immediately and all property and information belonging to the company that is in the vendor's possession should be returned.

Evaluating third-party vendor risks

A company has many risks that must be evaluated as part of a companywide compliance program. Therefore, it is essential a company has a process to identify which risks require additional attention and commitment of resources. With respect to third-party vendors, one way to evaluate vendor risks is to use a balancing test that looks at two primary factors: the nature of vendor's specific business activity and the vendor's access to confidential business information. A third-party vendor with a low-risk business activity that does not have access to confidential information may be assigned to a low-risk tier. Whereas a vendor with a higher risk business activity or access to confidential business information may be assigned to a mid-level risk tier. (Note that some business activities—or access to highly confidential information—may justify a vendor being placed in a higher-risk tier.) And a vendor that has a high-risk business activity and access to confidential information may be assigned a higher risk tier.

By assigning third-party vendors to risk tiers, a company can tailor its compliance program to focus on the vendors more closely where there is a higher degree of risk to the company. This means that a company can require greater levels of diligence, contract review, and monitoring for high-risk vendors than is required for mid-level or low-risk vendors. Likewise, high-risk vendors may be subject to more routine audits, although mid- or low-risk vendors may be subject to sampling or more infrequent audits.

Lastly, if a company decides to use a tiered approach to evaluate third-party vendor risks, the tiering process should be subjected to regular review to ensure that vendors are appropriately grouped in the right tiers and adjusted as necessary.

Existing vendors relationships

To be clear, third-party compliance is not just focused on prospective relationships with vendors. Companies are expected to take affirmative steps to ensure that existing or historical third-party relationships do not have indices suggesting potential misconduct. This can burden a company that acquired another company with preexisting relationships with third-party vendors. Companies are addressing this risk in several ways, including a more extensive due diligence review of the third-party vendor relationships during the acquisition process or conducting audits of third-party vendors once the acquisition is finalized.

Conclusion

Regulators are increasing pressure on companies to manage third-party relationships as part of an effective compliance program. This means that to mitigate this risk, companies must be proactive in managing and monitoring all aspects of their third-party vendor relationships. Therefore, it is vital that companies routinely examine their existing compliance programs to make sure they satisfy the current guidance for what constitutes an effective third-party compliance program. CT

Endnotes

1. U.S. Department of Health & Human Services, Office of Inspector General, *Measuring Compliance Program Effectiveness: A Resource Guide*, HCCA–OIG Compliance Effectiveness Roundtable Meeting, January 17, 2017, https://oig.hhs.gov/documents/toolkits/928/HCCA-OIG-Resource-Guide.pdf.
2. American Hospital Association, "New Report Shows Regulatory Burden Overwhelming Providers, Diverting Clinicians from Patient Care," news release, October 25, 2017, https://www.aha.org/press-releases/2017-10-25-new-report-shows-regulatory-burden-overwhelming-providers-diverting.
3. U.S. Department of Justice Criminal Division, "Evaluation of Corporate Compliance Programs (Updated June 2020)," https://www.justice.gov/criminal-fraud/page/file/937501/download.

Takeaways

- An effective compliance program includes a robust review of third-party vendors.
- A compliance program must look at the entire life cycle of a third-party vendor relationship.
- An appropriate third-party vendor compliance program should include a business need, due diligence, contractual limitations of risks, onboarding, monitoring, and enforcement and a process to conclude the vendor relationship.
- A third-party vendor's business activity and access to confidential information may determine whether a company considers a vendor to be low-risk, medium-risk, or high-risk.
- A company can tailor its compliance program to focus on higher-risk vendors, but it still must ensure appropriate oversight over low- or mid-risk vendors.

Upcoming virtual events

Compliance education from the comfort of your home or office

Looking for more educational opportunities that can help you stay up to date on the latest in compliance? SCCE® & HCCA® is here to help. Like our in-person events, our virtual events are led by experienced professionals and offer guidance on the emerging trends, regulatory updates, and best practices practitioners need to succeed—across all industries! You'll also get the opportunity to earn live Compliance Certification Board (CCB)® continuing education units (CEUs). HCCA members receive discounts on SCCE events. All events take place in central time unless otherwise noted.

NEW! Sports, Compliance, and Ethics Conference

Understand key challenges and best practices in sports and gaming compliance and the relevant takeaways for compliance and ethics programs across all industries.

January 19, 2023

Compliance Risk Assessment and Management

Get guidance and insights from experienced compliance professionals on how to conduct more effective risk assessments.

February 22-23, 2023 (CET)
June 26-27, 2023
September 27-28, 2023
December 12-13, 2023

Creating Effective Compliance Training

Take an in-depth look at the core principles of a successful compliance and ethics training program.

February 15-16, 2023
June 21-22, 2023
November 1-2, 2023

NEW! Aerospace, Defense & Government Contracting Compliance & Ethics Conference

Stay on top of the complexities of this heavily regulated industry with guidance from experienced professionals.

February 21, 2023

Nonprofit Sector Compliance Conference

Learn how to navigate the unique and diverse compliance risks that challenge the nonprofit sector. May 23, 2023

Learn more

corporatecompliance.org/virtual

SCCE® Society of Corporate Compliance and Ethics

Medicaid attestation frustration

by Kelly M. Willenberg

State Medicaid plans are in the process of implementation for the Consolidated Appropriations Act, 2021. While it is understood that state Medicaid plans are realizing their responsibility in the Consolidated Appropriations Act, 2021, the process is laborious and unnecessary.

Many children's hospitals across the country are struggling with the number of Medicaid plans they serve. With no consistent process, and the Medicare rules already established around claims processing for drug and investigational device exemption (IDE) trials, it is not surprising there are questions surrounding the rollout. Sites are going back to the January 2021 documents, qualifying each subject with the attestation form, and the paperwork is immense.

Section 210 of the Consolidated Appropriations Act, 2021 (Public Law 116–260) amended section 1905(a) of the Social Security Act (the Act) by adding a new mandatory benefit for routine patient costs for items and services furnished in connection with participation by Medicaid beneficiaries in qualifying clinical trials. How is this different from the National Coverage Decisions (NCD) 310.1 or the process most sites currently have? According to the Centers for Medicare & Medicaid Services (CMS), a determination for coverage for an individual participating in a qualifying clinical trial "shall be expedited and completed within 72 hours" by the state plan after submission of the attestation form . . . "shall be made without limitation on the geographic location or network affiliation of the health care provider . . . shall be based on attestation . . . shall not require submission of the protocols of the qualifying clinical trial, or any other documentation that may be proprietary or determined by the Secretary" to be burdensome to provide.[1]

Last year, there was concern about Medicaid plans not covering conventional care (which is part of the NCD 310.1 but not in Section 210). Other significant questions were on IDE and sponsored studies which are not outlined in it either. With all the above in mind, why then must the principal investigator *and* the healthcare provider (if different) attest to the appropriateness of the qualified clinical trial in which the individual is participating, when it is already done per Medicare claims processing, IDE rules, and NCD 310.1? The amount of paperwork on site is massive, and, in many instances, the form must be faxed.

What should you do right now? At the bottom of the form, in very small print, CMS states: "Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to CMS, 7500 Security Blvd, Attn: Paperwork Reduction Act Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, MD 21244-1850."[2]

I suggest sending a letter regarding the enormous burden this has placed on your site. In my opinion, CMS needs to hear from all sites regarding this arduous process. CT

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

Endnotes

1. Consolidated Appropriations Act, 2021, Public Law 116–260, December 27, 2020, https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf.
2. Medicaid.gov, "Medicaid Attestation Form on the Appropriateness of the Qualified Clinical Trial, accessed October 31, 2022, https://www.medicaid.gov/resources-for-states/downloads/medicaid-attest-form.docx.

UNDERSTANDING INFORMATION BLOCKING AND THE EXPECTATIONS FOR HEALTHCARE ORGANIZATIONS

by Dawn Morgenstern

Dawn Morgenstern
MBA, CHPC, CCSFP
(dawn.morgenstern@clearwatercompliance.com, linkedin.com/in/dawn-morgenstern) is Director, Consulting Services at Clearwater Compliance LLC, Nashville, TN.

In April 2021, the 21st Century Cures Act Final Rule went into effect, prohibiting healthcare entities from information blocking to break down barriers that have historically limited patient access to electronic personal health information (ePHI). To allow entities an opportunity to phase in their compliance, the initial rollout of the rule only covered a subset of electronic health information (EHI). However, as of October 6, 2022, entities will be responsible for complying with information blocking as it applies to the full scope of EHI.

Information blocking may be the most important change to health information since HIPAA. However, it's important to point out that information blocking is not a HIPAA rule and applies to all healthcare providers—not just HIPAA-covered entities.

Information blocking relates to any practice that might interfere with access, exchange, or use of ePHI, including any designated record set, regardless if a covered entity maintains the group of records or if the records are maintained for a covered entity.

In short, with few exceptions, healthcare providers, tech vendors, health information exchanges, and health information networks (HIN) can't prevent EHI access. The rule assumes that if HIPAA permits a patient or any other entity or individual to access records, they should be given access without delay, using almost any technology the requester chooses. Those requests do not have to be event-triggered.

For healthcare providers, it's about knowing which practices are considered unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

If an organization fails to provide access, without delay, to a person permitted access under HIPAA and other laws, that may be considered information blocking.

The ultimate goal is to improve healthcare data flow and facilitate improved and coordinated patient care with more patient engagement in healthcare decisions.

Who must be compliant?

Information blocking affects three types of entities:

1. Healthcare providers (regardless of HIPAA status).
2. Health information exchanges (HIE) and HIN. This is broadly defined and can include any entity that helps two or more providers exchange data. It also applies to a HIPAA business associate if the associate has an exchange role.
3. Health IT developers who offer Certified Electronic Health Record Technology.

If any of these organizations are also HIPAA-covered entities, there is an expectation that they must comply with HIPAA and the rules of the 21st Century Cures Act. Healthcare providers who aren't HIPAA-covered entities must still comply with information blocking.

Exceptions to information blocking

There are two categories of exceptions applicable to information blocking: denial exceptions and approval, and process exceptions related to how requests are fulfilled.

There are eight specific exceptions, with complex implementation standards that allow providers to deny ePHI requests without being seen as information blocking. The following is an overview of those exceptions.

Denial exceptions

1. Preventing harm exception

The preventing harm exception recognizes that organizations may deny requests if doing so protects patients or others from harm. Therefore, it's essential to document the potential risk and harm that triggered the exception.

In using this exemption, healthcare providers must demonstrate:

- A reasonable belief that access denial would substantially reduce the risk of harm to a patient or another person that would otherwise occur if fulfilled.
- Denial must be no broader than necessary to substantially reduce the risk of harm.
- There are two ways to determine risk of harm. The first is on an individualized basis when a licensed healthcare professional (who has a current or prior clinician–patient relationship with the patient) is exercising professional judgment. The other way is from data known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.[1]

2. Privacy exception

The privacy exception recognizes that an organization should not be required to use or disclose ePHI in a way that state or federal privacy laws prohibit. Information blocking does not render those laws obsolete.

"To satisfy this exception, [an organization's] privacy-protective practice must meet at least one of the four sub-exceptions:

- "***Precondition not satisfied*:** If [an organization] is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use of EHI, [it] may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.
- "***Health IT developer of certified health IT not covered by HIPAA:*** If an [organization] is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, [it] may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.

If an organization fails to provide access, without delay, to a person permitted access under HIPAA and other laws, that may be considered information blocking.

- "***Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2):*** An [organization] that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.
- "***Respecting an individual's request not to share***

information: An [organization] may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met."[2]

This exception mirrors HIPAA Privacy Rule provisions about which ePHI patients can access.

It's worth noting that it could be considered information blocking if an organization encourages patients to allow their providers access but infer the patient should be more selective in agreeing to access for others.

3. Security exception

The security exception covers all legitimate security practices by organizations but does not prescribe a maximum level of security or dictate a one-size-fits-all approach.

It is not considered information blocking if an organization interferes with access to protect ePHI security.

For instance, a practice believes data release would compromise data security. If a request threatens patient information, the security exception may be applicable. This should be consistent, nondiscriminatory, and tailored to specific security threats. It doesn't cover practices that claim to promote security but are unreasonably broad and onerous. The security exception should not be a broad brush for request denials.

If an organization uses this exception, it must demonstrate that the denial is directly related to ePHI safeguarding based on specific security risks. That should include updated and relevant privacy and security policies. If those don't exist, the organization should implement those to help mitigate practices that could prohibit or delay ePHI data sharing.

4. Infeasibility exception

The infeasibility exception notes that legitimate challenges could limit an organization's ability to comply with a request. For example, the organization may not have—and may be unable to get—requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use.

An organization may deny a request if it is considered infeasible. Before applying this exception, see if other exceptions may be more appropriate. The infeasibility exception should cover issues outside of an organization's control.

The practice must meet one of the following conditions:

- "Uncontrollable events: [The organization] cannot fulfill the request for access, exchange, or use of [EHI] due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
- "Segmentation: [The organization] cannot fulfill the request for access, exchange, or use of [EHI] because [it] cannot unambiguously segment the requested [EHI].
- "Infeasibility under the circumstances: [The organization] demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances."[3]

If using this exception, the organization should provide a written response to the requester within 10 business days of getting the request, including why the request is infeasible.

5. Health IT performance exception

The health IT performance exception recognizes that it requires maintenance and sometimes improvements for health IT to perform properly and efficiently. This may require some health IT systems to go offline temporarily and can be for scheduled or unscheduled reasons.

The practice must:

1. "Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
2. "Be implemented in a consistent and non-discriminatory manner; and
3. "Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN."[4]

An organization may act against a third-party app that is negatively impacting the health IT's performance, provided that the practice is:

1. "For a period of time no longer than necessary to resolve any negative impacts;
2. "Implemented in a consistent and non-discriminatory manner; and
3. "Consistent with existing service level agreements, where applicable.

"If the unavailability is in response to a risk of harm or security risk, [the organization] must only comply with the Preventing Harm or Security Exception, as applicable."[5]

The IT performance exception is for those issues that temporarily prohibit access and should be used consistently and in a nondiscriminatory manner.

Approval and process exception examples

In addition to denial exceptions for the information blocking, there are also a few approval and process exception examples. These exceptions are related to how organizations fulfill access requests.

These exceptions may trigger actions that hinder requests rather than outright denying them.

6. Content and manner exception

The content and manner exception provides clarity and flexibility to organizations about the required content of an organization's response to a request for access and how the organization may fulfill the request. The organization must fulfill a request in any manner requested unless technically unable or if they cannot reach agreeable terms with the requester to satisfy the request.

Content condition considers the scope of the data involved in information blocking. If the request is outside the scope, it would not be information blocking if the organization doesn't provide the data. Manner condition considers how the organization must fulfill an access request to satisfy the exception. Here, suppose the organization can't technically meet the request in the manner requested or can't reach agreeable terms with the requester. In that case, it may be necessary to fulfill the request in an alternative manner.

7. Fees exception

The fees exception enables organizations to charge fees related to technology development and service provisions that enhance interoperability. For instance, if the request comes from an attorney or life insurance agency and the organization currently charges a records request fee, that could likely continue. However, there are several requirements for fee basis, including anticompetitive, consistency, nondiscriminatory, and others, so organizations should review their current fee practices against these requirements to ensure the fees are allowable under the exception.

With the fees exception, it's important to note:

- You should not charge for records if HIPAA does not allow it.
- You should observe HIPAA limits.
- You should not change the policy to charge for records if it doesn't exist now.
- You should examine fee charges to determine if the process should continue.

Also, consider the "Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, Notice of Proposed Rulemaking," from January 21, 2021, that provides a summary of how different types of access and recipients of the PHI would affect the proposed allowable access fees.[6]

8. Licensing exception

Finally, the licensing exception allows organizations to protect the value of their innovations and charge reasonable royalties to earn returns on the investments they made to develop, maintain, and update those innovations. This often refers to electronic health records (EHRs).

The licensing exception allows vendors to continue to license technology without it being considered information blocking. Health IT developers that require licensing and licensing fees for interoperability components should understand that this exception could protect them if customers can't access information because they failed to license the necessary functionality.

The licensing exception protects intellectual property rights based on particular timing and licensing conditions.

Beyond understanding what information blocking is and which exceptions exist, it's also important to consider implementation.

Ensuring prompt access, exchange, and use

Beyond understanding what information blocking is and which exceptions exist, it's also important to consider implementation.

Compliant organizations should have well-defined processes to

evaluate and review requests, maintain documentation for compliance purposes and determine how denials are consistently tailored to one or more exceptions.

A playbook is an excellent foundation for implementation because it can help manage the convergence of people, processes, and technology to ensure reasonable and appropriate procedures and processes for compliance success.

People: Know who is asking for and responding to records requests and how.

- Identify organizational stakeholders related to information blocking.
- Start an information-blocking compliance workgroup. The workgroup should designate an organizational leader and consist of a multidisciplinary team of stakeholders such as legal, clinical, IT, and others to identify, assess, implement, and advocate for corporate compliance.
- Determine how to categorize and organize sharing and exchange. For example, does this require a technical solution or human intervention to process every request? Who within the organization is responsible for responding to requests?
- Discover and assess vendors that exchange, use, or access ePHI on the organization's behalf, request confirmation of the vendor's compliance program, and confirm that the vendor does not engage in information blocking.
- Identify requester types. Not all requesters are treated the same under the rules, and most organizations categorize request types and requesters. Requesters may be individuals (adults or minors), personal/legal representatives, or other providers.

Processes: Assess current access processes to determine gaps or compliance issues.

- Evaluate HIPAA policies and procedures to determine if they're up to date and functioning.
- Review, update, or create organizational policies, procedures, and processes for compliance.
- Revise policies that knowingly delay disclosure.
- Identify which new policies to create to document exceptions.
- Monitor privacy practices and look for improvement opportunities.
- Determine whether current access, exchange, or use rules and processes are "enough" to avoid the implication of information blocking.
- Decide when refusals are currently permitted and if those instances are still valid under the information blocking framework.
- Conduct a legal review of contracts, business associate agreements, data use agreements, or licenses.
- Understand that business associates who assist with record release or transfer may need additional instruction.
- Review and amend, as necessary, contracts and agreements that impose restrictions on the other party's access, exchange, or use of ePHI for compliance with the regulatory exceptions.
- Determine incident management processes and procedures. For example, how to handle a request when it can't be immediately provided.
- Implement a complaint process for reporting information-blocking complaints.
- Monitor, investigate, and enforce compliance through risk assessments and investigations.
- Train workforce members on information-blocking compliance.
- Remediate any issues, including implementing Consumer Assistance Programs and disciplinary actions for those who violate the policies.
- Consider combining information-blocking training with HIPAA compliance training.

Technology: Understand the technology required to respond to records requests.

- Determine the organization's capability to readily accommodate various electronic access methods.
- Assess all points of access and exchange, including technology and application programming interfaces (APIs) in use.
- Conduct a risk analysis of the new system or application implementations.
- Determine whether an exchange with a particular application creates too much risk.
- Remediate technical vulnerabilities, test APIs and infrastructure, and monitor the environment.
- Discuss upgrades or settings with EHR vendors.
- Understand patient portal capabilities.
- Understand which APIs vendors supply.
- Review protocols and data streams to ensure no unintentional blocking occurs.
- Identify other electronic data transfer mechanisms.

Information blocking and exceptions policy

Organizations must draft an information blocking and exceptions policy to ensure compliance with information blocking regulations. Because of

the overlap with HIPAA issues, it may be helpful to consider including this new policy as an addendum to current HIPAA policies and procedures.

These policies should establish well-defined processes that demonstrate the organization's ability to:

- Evaluate and review requests.
- Maintain documentation for compliance purposes.
- Determine how denials are consistently tailored to one or more of the information blocking exceptions.

Also consider:

- Putting exceptions into written policies.
- Paying attention to extensive criteria for each exception.
- Crosswalking with HIPAA policies.
- Conducting an internal analysis may require multidisciplinary input (clinical, legal/compliance, health information management, information systems, information security, etc.).
- Understanding that exceptions require application in a nondiscriminatory manner for like-requesters to stop providers from favoring their own systems or blocking out competitors.
- Drilling down to assess operations, policies, and practices. There is not a one-size-fits-all situation. CT

With few exceptions, healthcare providers, tech vendors, health information exchanges, and health information networks can't prevent ePHI access.

Endnotes

1. Office of the National Coordinator for Health Information Technology, "Cures Act Final Rule: Information Blocking Exceptions," last accessed October 21, 2022, https://www.healthit.gov/cures/sites/default/files/cures/2020-03/InformationBlockingExceptions.pdf.
2. Office of the National Coordinator for Health Information Technology, "Cures Act Final Rule: Information Blocking Exceptions."
3. Office of the National Coordinator for Health Information Technology, "Cures Act Final Rule: Information Blocking Exceptions."
4. Office of the National Coordinator for Health Information Technology, "Cures Act Final Rule: Information Blocking Exceptions."
5. Office of the National Coordinator for Health Information Technology, "Cures Act Final Rule: Information Blocking Exceptions."
6. Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, Notice of Proposed Rulemaking, 86 Fed. Reg. 6,446, January, 21, 2021, https://www.govinfo.gov/content/pkg/FR-2021-01-21/pdf/2020-27157.pdf.

Takeaways

- With few exceptions, healthcare providers, tech vendors, health information exchanges, and health information networks can't prevent electronic personal health information (ePHI) access.
- Information blocking assumes that if HIPAA permits a patient or any other entity or individual to access records, they should be given access without delay, using almost any technology the requester chooses. Those requests do not have to be event-triggered.
- HIPAA-covered entities are expected to comply with HIPAA and the rules of the 21st Century Cures Act.
- There are eight specific exceptions to the rule, with complex implementation standards allowing providers to deny ePHI requests without being considered information blocking.
- Organizations should have well-defined processes to evaluate and review requests, maintain documentation for compliance purposes, and determine how denials are consistently tailored to one or more exceptions.

REDUCE OCR ENFORCEMENT: GET RECOGNIZED CYBERSECURITY PRACTICES IN PLACE

by Kelly McLendon and Christopher Lyons

Kelly McLendon
RHIA, CHPS
(kmclendon@complianceprosolutions.com, bit.ly/linked-in-KellyMclendon) is Senior Vice President Compliance and Regulatory Affairs at CompliancePro Solutions, a wholly owned subsidiary of Genzeon LLC, Exton, PA.

Christopher Lyons
CISSP, HCISPP
(bnl41200@yahoo.com, linkedin.com/in/cmlyons), Director of Cybersecurity at CompliancePro Solutions, a wholly owned subsidiary of Genzeon LLC, Exton, PA.

Cybersecurity has continued to evolve across all public and private sectors that rely on digital personal information. This would typically be patient information in American healthcare under the U.S. Department of Health & Human Services (HHS) purview. HHS has taken a leadership role in coordinating efforts to align industry cybersecurity practices, which will strengthen defenses against ever-increasing (external and internal) cyberattacks. A new amendment to Health Information Technology for Economic and Clinical Health (HITECH) Act provides regulatory enforcement incentives to entities that use (for at least 12 consecutive months) recognized security practices, such as those to be subsequently discussed.[1] These incentives target covered entities and business associates subject to the HIPAA Security Rule. HHS recommends adopting recognized cybersecurity practices that can reduce liability under regulations already in effect—particularly the HIPAA Security Rule—but stop short of being safe harbors or providing formal regulatory relief.

As ransomware and other forms of malware and cyberattacks have increased, there have been several initiatives from the US government and the private sector to combat these trends. Rules have been issued, education content released, reminders circulated, and notices of enforcement for failure to adequately institute protective safeguards ramped up.

Federal agencies such as the Office for Civil Rights (OCR) and the Federal Trade Commission, among many others, have increasingly offered content such as educational materials while at the same time pressing enforcement actions meant to show that the regulators are serious about compliance with their rules. These actions use regulatory enforcement as incentives to tighten IT security to better arm these businesses to fight what has become, in essence, cyberwarfare between many bad actors, including those that are state-sponsored or protected and the vast numbers of healthcare providers, payers, exchanges, and networks. Added to those issues is the problem of insiders within the systems with protected or sensitive information who are malicious in intent.

405(d) and health industry cybersecurity practices (HICP) provide useful tools for cybersecurity programs

Across the world, bad actors (external and internal) are regularly identifying new and unique methods to probe for vulnerabilities in networks and applications to identify weak spots or flaws to access confidential data, trade secrets, or conduct other nefarious activities. Their efforts yield a constant barrage against entire systems and networks, looking for weaknesses they may exploit. The methods used are continuously adapting to meet new security controls implemented by businesses.

While the methods evolve, many of the exploits have stayed the same—either with some changes or sometimes without the need to change. Methods such as social engineering are not new; however, they are still exploitable as many companies still need to employ the systems or methods identified to eliminate these older methods. Ransomware and phishing are two of the most common forms of attack today. Efforts such as the HICP-recommended cybersecurity practices can help to expand and standardize what practices and controls should be considered by any organization for cyberdefense.

According to the HHS "Fact Sheet: Cybersecurity Act of 2015, Section 405(d)," "in 2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 150 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts."[2]

The 405(d) Task Force executed its mission by examining existing US cybersecurity safeguards, protections, controls, and practices, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). However, in a somewhat simplified form and with an added dimension, they tailored the controls and practices into three versions based on organizational size (small, medium, or large), providing a sample definition of each. This new framework will greatly help companies of all sizes apply industry-accepted practices using a well-established CSF such as the NIST CSF within their environment, regardless of size or complexity.

The 405(d) Task Group agreed on developing HICP components: a main document, two technical volumes based on organizational size, and a robust appendix of resources and templates:[3]

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates
- Cybersecurity Practices Assessments Toolkit (Appendix E-1)

With these published tools, including end-user training content, a physician's practice can clearly see which cybersecurity controls and practices should or could be used for their small-sized business and use coordinated content to train its workforce. The same is true for a middle-sized network of offices or clinics as well as larger entities such as hospitals. Other entities, such as payers and business associate vendors, can also choose size based on their own interpretation of the intent of the practices.

Efforts such as the HICP-recommended cybersecurity practices can help to expand and standardize what practices and controls should be considered by any organization for cyberdefense.

Threats and cybersecurity practices

HICP identified and published five main areas of high threat to health information and patient safety. Each of these threat areas is the focus of the following recommended practices.[4] Differing controls and practices are employed against the threats requiring IT sophistication to analyze and determine how to use with systems and cybersecurity technologies.

1. Insider, accidental, or intentional data loss
2. Loss or theft of equipment or data
3. Email phishing
4. Ransomware
5. Attacks against connected medical devices

HICP also identified 10 recommended—not prescribed—cybersecurity practices tailored to fit small, medium, and large organizations, as illustrated and supported in detail within Technical Volumes 1 and 2. The 405(d) Task Force emphasizes that these are not required practices but rather a roadmap and highly desirable voluntary set of practices that can and should be analyzed and adapted according to each entity's security plan.

1. E-mail protection systems
2. Endpoint protection systems
3. Access management
4. Data protection and loss prevention
5. Asset management
6. Network management
7. Vulnerability management
8. Incident response
9. Medical device security
10. Cybersecurity policies

405(d)/HICP and HIPAA Security Rule compliance

It should be noted that the 405(d) practices do not address all areas of the HIPAA Security Rule and should be considered to work with the Security Rule requirements. 405(d) provides a different level of detail that can form increased HIPAA and recommended cybersecurity practice compliance. It is important to always comply with the requirements of HIPAA, but now combine that compliance with appropriate cybersecurity practices to lessen risk on several fronts.

These are the areas addressed within HIPAA but are excluded from the HICP published practices:

- Compliance administration and governance
- Education and training
- Auditing and monitoring
- Vendor management
- Other HIPAA controls

HITECH is amended

In January 2021, Congress amended HITECH by adding a few paragraphs which are of great significance. If recognized security practices have been in place for no less than 12 months, there can be a lessening of enforcement in areas such as fines, length of audits, and positively be considered in relation to other remedies that may be imposed for HIPAA Security Rule violations.

As with most laws the subsequent rule-making may further clarify this new HITECH update, but the meaning is straightforward, adopt and implement recognized security practices and lighten the risk of negative enforcement action. Although the update also makes clear that this in no way eliminates enforcement, rather executing such practices will allow the company to have a better opportunity to

lower the investigation process, penalty, and other remedies, such as corrective action plans.

The ability to lessen the impact of a breach is a good reason to apply such practices; the risk to patient data outweighs everything else, which is the major reason for incorporating these practices. 405(d) has been identified as a recognized security practice. At the time of this writing, HHS has signaled that they will publish more content about what "recognized security practices" may be used.

What are "recognized security practices?" According to the update, it means "the standards, guidelines, best practices, methodologies, procedures, and processes developed . . . National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security Rule."[5] This last sentence illustrates that cybersecurity practices and control must work within a HIPAA Security Complaint Rule plan.

Lessening risk

Risks and liabilities from successful, bad actor (including insiders) practices with malware, phishing, ransomware, etc., are reduced by using the recommended practices as tailored for your entity—not just from regulators, such as OCR, but also for civil liability (from lawsuits and similar legal actions) as well as cyber insurance purposes.[6] HICP has published a helpful document about cyber insurance, and the impact cybersecurity practices can have. This has been borne out by recognition by the insurance industry that their customers must execute appropriate cybersecurity measures which tend to align with the HICP practices.

HHS has clearly stated, and it seems obvious, that it is time to implement a form of recognized cybersecurity practices! CT

Endnotes

1. An Amendment to Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 116–321, 134 Stat. 5072 (2021), https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.
2. U.S. Department of Health & Human Services, Office of the Chief Information Officer, "Fact Sheet: Cybersecurity Act of 2015, Section 405(d),"Fall 2018, https://www.nist.gov/system/files/documents/2018/10/18/hhs_fact_sheet_-_csa_405d_cleared.pdf.
3. U.S. Health & Human Services, "HHS 405(d) Aligning Health Care Industry Security Approaches: Resources," accessed November 1, 2022, https://405d.hhs.gov/resources.
4. 405(d) Task Group, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, accessed November 1, 2022, https://405d.hhs.gov/Documents/HICP-Main-508.pdf.
5. An Amendment to Health Information Technology for Economic and Clinical Health Act.
6. Traci Lamb and Mitch Parker, "A Word from the Task Group: Cyber Insurance—From Risk Transference to Organizational Assurance," *The 405(d) Post*, vol. 16, May 2022, https://405d.hhs.gov/Documents/405d-post-volxvi-2022-may.pdf.

Takeaways

- Health Industry Cybersecurity Practices (HICP) is a public–private partnership formed as the result of federal law that has produced cybersecurity tools for small, medium, and large organizations.
- The 405(d) cybersecurity practices are drawn from the National Institute of Standards and Technology Cybersecurity Framework.
- Cybersecurity protections for patient information have become so important that the federal government has amended Health Information Technology for Economic and Clinical Health to allow the Office of Civil Rights to favorably view an organization's "recognized security practices."
- Liability is rising across several fronts from civil lawsuits to cyber insurance and regulators requiring increased cyber diligence.
- HICP has identified five threats and 10 recommended cybersecurity practices tailored to organizational size.

Let's stay connected!

Follow HCCA on social media:

- Keep up with industry trends
- Stay up to date on healthcare compliance news
- Learn about upcoming conferences and events

Find us on:

Connect with us
hcca-info.org/socialnetworks

HCCA
Health Care Compliance Association

Nonverbal communication matters

by Donna Schneider

Tip #6: Things to be aware of when having the crucial conversation: In-person versus remote with camera matters

Much of our focus over the past few months has been on how to enhance dialogue during a compliance conversation. We have spent time on verbal signals and words that can improve effectiveness. However, there is another component to conversation: nonverbal communication. Nonverbal cues during conversations matter because these signals tell a visual story of the conversation. Cues are signals that conversation participants absorb through seeing your nonverbal expressions and/or body language. This happens during in-person discussions as well as conversations held virtually through a computer screen.

According to Vanessa Van Edwards in her book *Cues: Master the Secret Language of Charismatic Communication*, you can have the best content in the world, but if it is not shared with the right charisma cues, it doesn't land.[1] Cues for warmth, charisma, and competence are nonverbal signals that can increase the confidence your conversation partner has in you. Similarly, there are also nonverbal communications that can decrease affinity and confidence. We must navigate both in-person and virtual communication venues, so paying attention to nonverbal communication is critical to a successful conversation. Building warmth, competence, and charisma cues with your conversation participant can enhance the flow of dialogue.

Examples of inviting nonverbal communication cues included tilting your head, nodding, and raising your eyebrows in agreement. Charisma cues can be incorporated into the conversation by leaning in toward the person you are speaking with or the computer screen and focusing on facing the person directly when speaking in person or on the screen if virtual. Lastly, competence cues are another form of nonverbal communication and include actions like displaying your palms when explaining something or making a steeple out of your fingers. Be wary of your facial expressions, however. Attempt to consciously avoid pursing your lips or looking away from the person you are having a conversation with, whether in person or virtually. Those can destroy dialogue no matter what words are being said.[2]

I encourage you to try the warmth, charisma, and competence cues in the mirror when practicing for a conversation. If you use those, you should see an increase in connection with your conversation partners. It can only enhance the quality of the dialogue and the free flow of information, which is what you are seeking during a compliance conversation. CT

Donna Schneider
RN, MBA, CPHQ, CPC-P, CHC, CPCO, CHPC, CCEP
(dschneider@lifespan.org) is Vice President, Corporate Compliance and Internal Audit, Chief Compliance & Privacy Officer at Lifespan, Providence, RI.

This column focuses on useful tips the author has used to work through difficult conversations efficiently, effectively, and without emotion to determine the truth.

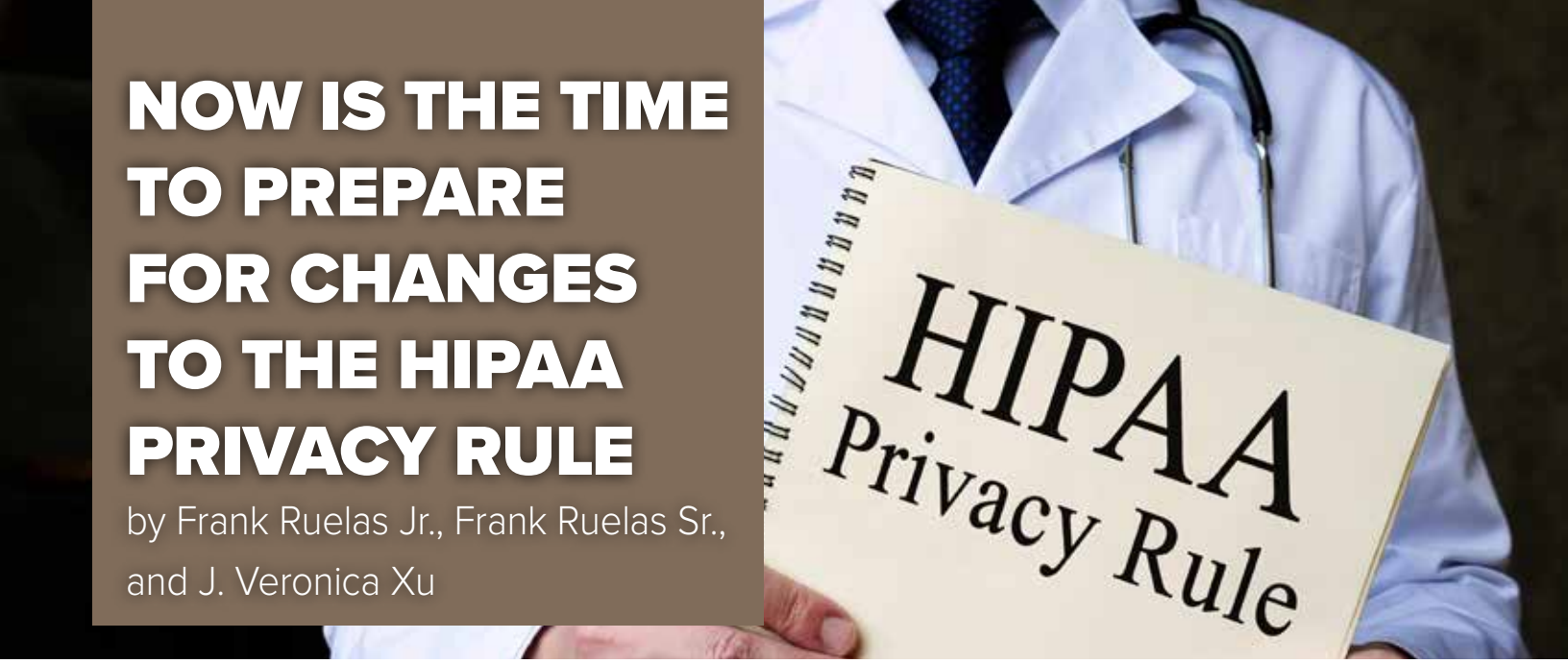
This is the final "Let's talk" column. We want to thank Donna Schneider for her contributions to Compliance Today.

Endnotes

1. Vanessa Van Edwards, *Cues: Master the Secret Language of Charismatic Communication*, (New York: Random House Penguin, 2022), 15.
2. Van Edwards, *Cues*, 158.

NOW IS THE TIME TO PREPARE FOR CHANGES TO THE HIPAA PRIVACY RULE

by Frank Ruelas Jr., Frank Ruelas Sr., and J. Veronica Xu



Frank Ruelas Jr.
(frank@compliacademy.com) is Compliance Manager at PCP of AZ.

Frank Ruelas Sr.
(francisco.ruelas@commonspirit.org) is Corporate Responsibility Officer at SJHMC/SJWMC, CommonSpirit Health.

J. Veronica Xu
(veronica.xu@saberhealth.com) is Chief Compliance Officer at Saber Healthcare Group.

According to the Office of Information and Regulatory Affairs, Office of Management and Budget, final action on the proposed rules—published in the *Federal Register*—to modify the HIPAA Privacy Rule is scheduled to occur in March 2023.[1] Compliance professionals may want to take advantage of the lead time to prepare for possible changes to the Privacy Rule before the final rules are published in the *Federal Register* and, in particular, designated privacy officials responsible for developing and implementing policies with respect to the Privacy Rule. This lead time can allow privacy officials to take important steps to help transition their organizations from their current state of compliance with the Privacy Rule to the future state of compliance with the new requirements.

Even though we will not know precisely the specific changes to the Privacy Rule until the final rule is published in the *Federal Register*, the Notice of Proposed Rulemaking issued in January 2021 provides a useful perspective on what changes we may expect to see in the final rule.[2] This advance notice can provide a convenient and manageable time frame for individuals to assess and develop processes and workflows without the high pressure of working under a short timeline.

With respect to time, it is imperative that privacy officials also know that whenever the final rule is published, covered entities will have 240 days after the publication of the final rule before enforcement begins. Despite that, starting preparation as soon as possible provides more time to address the challenges we will face once the final rule takes effect. And although the government agency has yet to publish the final rule, such uncertainty should not be used as an excuse to do nothing, and covered entities should take preparatory actions early since previously proposed HIPAA rules often closely resemble the finalized ones with minor or no revisions. To help privacy officials plan and prepare for the upcoming changes, the following steps are provided for fellow compliance professionals' consideration.

Identify the possible future state

To begin preparation, it is vital to first review the proposed changes to the HIPAA Privacy Rule and identify the gaps between the proposed rules and your current processes, policies, and practices. The January 21, 2021, *Federal Register* and the notice of proposed rulemaking detailed the specific changes that will come our way.[3] To help navigate through the different sections describing the proposed rules, there is a table

of contents on the first page, which is organized into five main sections. The third section, titled "III. Need for the Proposed Rule and Proposed Modifications," outlines detailed revisions that are expected to be finalized in March 2023.

Interestingly, one can make an anecdotal conclusion on which of the sections of the Privacy Rule may be affected most significantly. Using this approach, the section dealing with an individual's access to protected health information (PHI) is the most extensive section where proposed changes appear in the Notice of Proposed Rulemaking (NPRM). When considering the ongoing focus and communications by the U.S. Department of Health & Human Services Office for Civil Rights (OCR) on the importance of providing an individual with access to PHI maintained in a designated record set, it is likely that this is also the section within the Privacy Rule that will be affected the most by the proposed changes listed in the notice of proposed rulemaking.

Second, become familiar with the changes in the NPRM; take advantage of the fact sheet related to the proposed rules, which OCR posted on December 10, 2020.[4] This six-page document is a summary of the proposed changes listed in the NPRM. The fact sheet also makes it easier to cross-reference the summary of proposed changes to the more detailed content of the proposed changes that appear in the *Federal Register*. This is also a good reason why having both documents—the *Federal Register* and fact sheet—can be instrumental in developing a comprehensive and detailed understanding of the proposed changes.

Connecting the current state to the future state

By becoming acquainted with the proposed changes, privacy officials can then take steps to identify how the current state compares with some of the specific and possible modifications presented in the final rule. Because of certain significant modifications proposed in the final rule, all pertinent policies and procedures must be reviewed and updated accordingly. It is essential to start the review process and begin the dialogue with policy owners so that they become aware of and familiar with the upcoming changes. By collaborating with them, privacy officials can receive valuable feedback and insights on the potential challenges and impact the new rule may impose on the organization's processes and practices. The following are a few examples of the proposed new rule, its potential impact, and its respective workflows.

In the current rule, under the requirements for PHI access, a covered entity must act upon a request for access no later than 30 days after receipt of the request. In the proposed rule, the suggested change is to shorten the time frame from 30 to 15 days after receipt of the request for PHI access. Essentially, this proposed change is moving from a current state of 30 days to respond to a request for access to a future state of 15 days.

Given this proposed change, the privacy official may decide to connect and discuss with those process owners who manage the response time to requests to access PHI. For instance, is there data to show the current number of days that the covered entity responds to requests for access to PHI? Do the process and policy owners see the change from a 30-day response time to a 15-day response time as problematic? If so, what are some strategies that may need to be considered so that the covered entity can comply with the proposed 15-day time frame in responding to requests to access PHI? These are just a few questions that need to be asked and answered. Collaborating with those responsible for handling requests for access to PHI and completing this thought exercise can help covered entities identify possible options and maximize the time needed for necessary changes to the current process.

Because of certain significant modifications proposed in the final rule, all pertinent policies and procedures must be reviewed and updated accordingly.

Policy management

If the covered entity's access to the PHI process is also codified in a policy and procedure, this is another "to-do" item on the task list that the privacy official may need to prepare for. For example, some organizations may review their Privacy Rule-related policies and procedures every two or three years. When the final rule is published, it will be crucial that the current policies and procedures be reviewed and updated promptly

to ensure their consistency with the law. What is important to do in such a situation is to also make sure that whatever system is used to track and monitor when policies are reviewed is updated to reflect when the next review of these policies will occur. Many policy management systems include functions that allow for policies and procedures to be logged and send a notification to policy owners and reviewers when a particular policy and procedure is due for review. This may also be a good time to verify that the list of current policy owners responsible for the review and policies is still accurate, as personnel changes may have occurred since the last time various policies and procedures were reviewed.

Reviewing and revising policies also presents another opportunity for privacy officials. They can use this opportunity to assess how easy it is for the workforce to access the affected policies. To maintain an effective compliance program, it is important that the policies are made readily available, and the workforce can easily access policies whenever needed, which will, in turn, increase the chance of timely application of policies in practice as well as the level of compliance.

New requirements

Along with changes to various sections within the current HIPAA Privacy Rule, the proposed rules also introduce new requirements related to new sections that may become finalized when the final rule is published. Now is an excellent time to look at some of these requirements and start identifying who would be good partners to begin assessing what actions will be needed to meet the new requirements. Consider the example of the newly proposed section 45 C.F.R. § 164.525, which deals with medical record requests.

The proposed rules introduce a new section in the Privacy Rule that lists several new requirements if a covered entity has decided to impose fees related to specific requests for medical records. These requirements include posting a fee schedule on the covered entity's website and making the fee schedule available upon request and at the point of service.

Looking closely at the requirements of this new proposed section on medical records fees, a privacy official may identify other people within the organization who need to be involved in planning for these changes. It would include the individuals who maintain the covered entity's website, medical records staff that are aware of and apply fee schedules related to medical record requests, and the staff that

interacts with patients who may request a copy of their medical records. In addition, processes will need to be developed to respond timely to fee schedules requests, provide an individualized estimate of the approximate fees related to a specific request for medical records, and determine when it is allowable to impose a cost-based fee associated with the type of request received for medical records. Since the fees are based on specific cost items related to labor, supplies, and postage, there will also need to be a process to calculate these costs so that the estimated fees are a good approximation of what may be imposed upon an individual. As such, this is a good example of how the proposed rules will require a team effort to work toward reaching compliance; it is unlikely that any one person would be expected to perform the necessary changes that the proposed rules may bring about.

Third-party partners or resources

The third suggested area to consider in preparing for the proposed changes involves connecting with third-party partners or resources. For this, the example of revising and reprinting the covered entity's Notice of Privacy Practices (NoPP) is used, given that the proposed rules will introduce material changes to the covered entity's privacy practices. As such, covered entities will need to replace their current versions of their NoPPs prominently displayed in areas where individuals receiving care are expected to see them.

For some covered entities, this may be as straightforward as working with an internal department, such as a print shop, to request new NoPPs. For other others, an external resource may be what is used to order and receive revised NoPPs. In either case, the privacy official or another person responsible for obtaining the NoPPs for display should identify the contact person to arrange for ordering new NoPPs. This provides an opportunity to determine what costs will be involved, the turnaround time for the new NoPPs to be delivered, and the process of ordering new NoPPs. However, there is another opportunity that the need for ordering revised NoPPs also presents, which can be very useful in promoting compliance with the HIPAA Privacy Rule.

It is not uncommon for NoPPs to go missing or unaccounted for. For instance, if the waiting room where a NoPP is posted goes through any remodeling, it may mean that the NoPPs are taken down but sometimes not replaced—for whatever reason—after the remodeling is completed. In addition, the privacy official can also ensure that since the last NoPPs were distributed and posted, there are no new areas to consider for placing a copy of the NoPP. For example, a new NoPP may be needed for the waiting room in a newly established outpatient department that was put into operation since the last time NoPPs were installed. This enables the privacy official to confirm the locations of NoPPs that need to be replaced and also gives them the opportunity to identify new spots for NoPPs that may not have existed in the past.

It is unlikely that any one person would be expected to perform the necessary changes that the proposed rules may bring about.

Conclusion

Changes to the HIPAA Privacy Rule requirements do not occur very often. So, when changes are expected, it is imperative to take advantage of a plan to identify possible changes and how they will impact current processes or introduce the need for new processes. Fortunately, concerning the proposed changes to the Privacy Rule, compliance professionals can take advantage of the time available from the date that the final rules are published to the day that enforcement of the final rules will begin. CT

Endnotes

1. Reginfo.gov, "View Rule: HIPPA Privacy: Changes to Support, and Remove Barriers to, Coordinated Care and Individual Engagement," Spring 2022, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=0945-AA00.
2. Proposed Modifications to the HIPPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Fed. Reg. 6,446 (January 22, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-21/pdf/2020-27157.pdf.
3. Proposed Modifications to the HIPPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual.
4. U.S. Department of Health & Human Services, Office for Civil Rights, "Office for Civil Rights (OCR) Proposed Modification to the HIPAA Privacy Rule to Empower Individuals, Improve Coordinated Care, and Reduce Regulatory Burdens FACT SHEET," December 10, 2020, https://www.hhs.gov/sites/default/files/hipaa-nprm-factsheet.pdf.

Takeaways

- Currently, the final rule for modifications to HIPAA is expected to be published in March 2023.
- The proposed rules strengthen several key aspects related to an individual's right to access protected health information.
- New requirements that may be finalized include providing individuals with estimates on fees regarding requests for copies of medical records.
- Individuals designated with the responsibility of implementing HIPAA privacy policies may want to consider creating work teams to begin assessing the impact of the proposed changes to the Privacy Rule.
- Covered entities will have 240 days from when the final rule on modifications to the Privacy Rule is published in the *Federal Register* to prepare for enforcement.

Don’t miss out on this opportunity - Save your spot today!

Managed Care Compliance Conference

January 31 – February 2, 2023 | Virtual

Join us for our annual event dedicated to compliance management for health plan providers. Learn the latest best practices and emerging trends from industry leaders while making connections with peers and mentors who understand the day-to-day issues and strategies specific to the managed care environment.

Topics include:

- Navigating OIG Oversight
- Cybersecurity and Managing Cyber Risk
- Updates on Mental Health Parity Enforcement
- 2023 Regulatory Changes
- Creating Effective & Engaging Compliance Training
- Best Practices in Medicare Compliance
- CMS Program Audit Strategies

What attendees are saying:

“The information was pertinent to managed care, it was interesting and gave great insight into how we can improve our organization.”

“Learning about managed care compliance in different settings (not just the big health insurance companies).”

“Very knowledgeable presenters with a wide array of topics covered. The HCCA staff are helpful and the entire conference – from an attendee perspective – was very smooth. Well done.”

Learn more
hcca-info.org/2023managedcare

HCCA
Health Care Compliance Association

POST-ACUTE CARE PROVIDERS' FRAUD RISKS

by Randi Seigel and Krusheeta R. Patel

Randi Seigel

(rseigel@manatt.com; @RSeigz; bit.ly/linked-in-RandiSeigel) is Manatt Health Partner at Manatt, Phelps & Phillips LLP, New York, NY.

Krusheeta R. Patel

(kpatel@manatt.com; linkedin.com/in/krusheeta-patel/) is Manatt Health Associate at Manatt, Phelps & Phillips LLP, New York, NY.

Like other healthcare providers, post-acute care (PAC) providers—specifically skilled nursing facilities (SNFs), home health agencies (HHAs), and hospice providers (collectively referred to in this article as "PAC providers")—have long faced significant regulatory burdens to ensure compliance with myriad Medicare and Medicaid conditions of participation and conditions of payment (CoPs). Because physicians and nonphysician practitioners are the gatekeepers for many PAC services, PAC providers often rely on unaffiliated physicians and nonphysician practitioners to certify a patient's eligibility for services. This is in addition to overseeing a plan of care and obtaining necessary documentation in the time frames required by the CoPs—which can be challenging. Additionally, PAC providers rely more heavily on referrals from hospitals, physicians, and other community providers than different types of acute care or specialty providers; this greater reliance on opportunities from referral relationships presents more substantial fraud, waste, and abuse concerns.

To understand the current risk areas—many of which are the same that have existed for decades—it is important to understand the history of scrutiny of these PAC providers, which is where this article begins. We then discuss current risk areas and recent government activity in those areas and, finally, where we anticipate ongoing or increased scrutiny.

History of government scrutiny

The federal government has long viewed PAC providers as high risk for engaging in fraudulent and abusive conduct. Many early U.S. Department of Health & Human Services, Office of Inspector General (OIG) Special Fraud Alerts focused on PAC providers. In 1995, the OIG issued a Special Fraud Alert focused on HHAs engaging in several concerning activities, including billing for services not provided; paying kickbacks to referral sources, including physicians, SNFs, and senior living facilities, for referring patients to the agency; and physicians certifying patients as eligible for homecare who are not eligible.[1]

In 1996 and 1998, OIG issued two separate Special Fraud Alerts focused on SNFs: one related to providers rendering services to SNF residents billing for services not provided[2] and the other related specifically to SNF relationships with hospice providers.[3] The latter relationships

are particularly vulnerable to fraud and abuse because SNFs provide a sizeable pool of potential hospice patients. SNF hospice patients often have longer lengths of stay, which may require fewer services, making them more profitable than patients who reside at home.

As hospice utilization and spending has grown, OIG has shifted attention to the vulnerabilities in this program. In particular, OIG has identified fraud schemes to recruit patients who may not be eligible for hospice and billing for a higher level of care than necessary.

Home health

Home health providers have paid at least $422.6 million since 2012 to settle False Claims Act (FCA) allegations. This represents 51 different cases from 2012 to 2020.[4] In 2021, Medicaid Fraud Control Units brought 39 criminal and 28 civil actions against HHAs, resulting in $176 million and $18.4 million in recoveries, respectively.[5]

From January 2022 until August 2022, based on publicly available data, three home health providers have settled FCA allegations for a total of $7.66 million related to alleged lack of medical necessity, upcoding, and failure to return a known overpayment.

Hospice

Hospice providers have paid at least $254 million since 2012 to settle FCA allegations involving at least 37 hospice providers.

In 2021, the Medicaid Fraud Control Unit brought six criminal cases and one civil fraud case against hospice providers resulting in payment of $85,327,396, and there remained 100 open investigations against hospice providers.[6]

SNFs

SNFs have paid at least $45 million since 2012 to settle FCA allegations involving more than eight SNFs. Most of these settlements arose from alleged violations of the Anti-Kickback Statute (AKS).

At the end of 2021, there were 321 open investigations against nursing facilities for fraud.[7]

Current risk areas

PAC providers' risk areas remain generally related to inadvertent or unintentional documentation errors that can result in a PAC providers' receipt of an overpayment, which, if not promptly returned, can result in FCA liability. The federal FCA makes it illegal to knowingly present, or indirectly cause to be presented, a false or fraudulent claim for payment to the federal government.[8] The FCA does not require intent to defraud or "actual" knowledge.[9] Conduct constituting deliberate ignorance or reckless disregard can also land a PAC out of compliance with the FCA. Failure to promptly repay an overpayment can form the basis of a false claim prosecution under the FCA (Medicare and Medicaid providers have an obligation to report and return overpayments within 60 days of identification).[10]

Other risk areas include nefarious conduct, such as admitting or accepting patients who fail to meet Medicare or other payors' eligibility criteria or billing for services that were not provided.

False claims

Home health

HHAs continue to face liability for:

- Failure to meet Medicare eligibility criteria, such as the beneficiary not being homebound or not in need of skilled services
- Failure to document services provided
- Billing for services not actually provided

OIG audit continues to audit HHAs and finds that their patients fail to meet or the agency fails to document that the patients meet eligibility criteria.[11], [12]

In 2021, an audit report published by OIG estimated that an HHA overbilled Medicare by "at least $2.1 million" for, in part, failing to meet medical eligibility criteria.[13] In 2021, PruitHealth Inc., paid $4.2 million to settle FCA claims for failing to document medical eligibility requirements, such as a face-to-face certification, a plan of care, and homebound status, in accordance with requirements.[14]

The federal FCA makes it illegal to knowingly present, or indirectly cause to be presented, a false or fraudulent claim for payment to the federal government.

Hospice

Hospice providers continue to face liability for:

- Failure to obtain a signed certification from the patient's physician or the hospice's medical director of the patient's terminal condition
- Billing for a higher level of care than what is medically necessary

- Failure to obtain documentation of a face-to-face encounter with a hospice patient no more than 30 days prior to the third hospice benefit recertification period

In 2018, a Pennsylvania hospice care provider, SouthernCare Inc., paid over $5 million to resolve FCA allegations for claims involving "hospice care that was medically unnecessary or lacked documentation."[15] In 2020, a Florida hospice agreed to pay $3.2 million to settle allegations that it submitted claims for patients who were not terminally ill and billed for inpatient-level care when the higher level of care was not medically necessary.[16] In 2021, a hospice chain settled an FCA investigation for $5.5 million related to allegations that it provided hospice services to patients who were not terminally ill.[17]

In addition, hospices have faced scrutiny related to "unbundling" services from the hospice per diem rate. In a recent OIG report, following three prior OIG reports on the topic, the OIG identified $6.6 billion paid to nonhospice providers over 10 years for items and services provided to hospice beneficiaries—which potentially should have been included in the hospice benefit.[18] The report noted that 58% of the durable medical equipment, prosthetics, orthotics, and supplies claims were billed to Medicare in error and should have been included in the hospice per diem rate, which resulted in Medicare paying the claims twice.[19]

SNFs

SNFs continue to face liability for:

- The provision of substandard quality of care
- Billing for medically unnecessary treatment, including keeping residents in a SNF longer than needed
- Providing higher levels of rehabilitation therapy than medically necessary

In 2020, a hospice paid $9.5 million to resolve allegations that it violated the FCA by submitting claims for rehabilitation services that were not reasonable, necessary, or skilled, as well as creating false preadmission documentation.[20] In 2021, 11 SNFs in New York were prosecuted under the FCA for, among other allegations, keeping patients at the facilities and billing for their treatment for longer than was clinically indicated.[21] In 2021, a Georgia-based SNF paid $11.2 million to resolve allegations that it violated the FCA by billing Medicare and Medicaid for therapy services that were not reasonable and necessary and for providing grossly substandard care.[22]

A strong compliance program focused on the risk areas can mitigate FCA liability risks

PAC providers should regularly evaluate their intake and operational programs to ensure they have adequate controls in place to assess a patient's eligibility for admission and the level and type of services being provided. Compliance officers should verify monitoring and auditing related to longer-stay patients and residents to assess whether patients or residents continue to qualify for and need services. This requires audits that look not only at the necessary documentation but also the patients' conditions and diagnoses. This oversight will involve a partnership between the compliance and quality departments. If a PAC provider determines eligibility is questionable or documentation is missing, the provider must promptly return any overpayments to avoid FCA liability resulting from knowingly retaining an overpayment. Findings from monitoring and auditing activities should be tracked and trended over time to assess whether any systemic failures could result in greater fines and penalties.

In addition, hospice providers should assess how often nonhospice providers are rendering services to their patients and confirm there are protocols to evaluate whether the service should be billed to and paid for by the hospice or the Medicare program.

For SNFs, it's critical that the quality of care rendered to residents is constantly evaluated. SNFs should consider engaging a third party to perform such quality audits periodically and at least twice a year.

Anti-kickback risks

PAC providers have several referral channels through hospitals, community-based organizations, and individual physicians. Each of these present heightened risk under the federal AKS. Similarly, OIG has long viewed PAC providers' relationships with one another—as assisted living facilities and group homes are ripe for AKS violations.

The AKS makes it a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce or reward referrals of items or services reimbursable by federal healthcare programs.[23] "Remuneration" is defined as anything of value, whether offered or provided directly or indirectly, overtly or covertly, in cash or in kind. Courts have generally held that the AKS is violated if at least one purpose of payment is the improper inducement of referrals or the generation of federal healthcare program

business, even if there are other legitimate and lawful purposes for the payment. A violation of AKS constitutes a false claim.

PAC providers have been subject to countless enforcement actions related to violations of the AKS:

- In 2021, seven SNFs under common ownership and management were sued under FCA allegations relating to the SNFs entering "into medical directorship agreements with certain physicians that purported to provide compensation for administrative services, but in reality, were vehicles for the payment of kickbacks to induce the physicians to refer patients to the seven SNFs."[24]
- In 2021, a hospice provider in California was sentenced to 30 months in prison pursuant to a hospice fraud scheme in which a hospice paid illegal kickbacks to patient recruiters in exchange for the referral of hospice beneficiaries.[25]
- In 2021, an HHA paid $17 million to settle allegations that it violated the AKS, alleging that it paid a kickback to a retirement home operator by purchasing two of its HHAs to induce referrals from the retirement home operator.[26]
- In 2022, a patient recruiter pleaded guilty to paying kickbacks to Medicare beneficiaries to recruit them for referral to HHAs. In exchange for referring these beneficiaries, the patient recruiter allegedly solicited and received kickbacks and bribes from the HHAs.[27]

Reviewing financial relationships and marketing activities is critical to mitigating AKS risks

PAC providers should ensure their legal and compliance departments review all relationships with referral sources prior to implementing an arrangement. Specifically, PAC providers should evaluate whether they are furnishing a service to a referral source for free or below fair market value; this includes the provision of staff to perform a service on behalf of a referral source that would otherwise be a cost for the referral source. Anytime a PAC provider furnishes a social worker or other employee or contractor to assist a referral source with discharge planning, coordinating referrals should be carefully analyzed under the AKS. Additionally, PAC providers' contracts with medical directors should be reviewed by the provider's legal department, and there should be ongoing monitoring to confirm that the medical directors are actually providing valuable services for which they are being paid. Lastly, any proposal to offer gifts, travel, tickets, or other items to a referral source should be considered suspect and analyzed to evaluate the risks under the AKS. Compliance departments may want to review large shifts in referral patterns to understand the basis for the shift and determine whether any remuneration flows from the PAC provider to the referral source.

What is on the horizon for PAC compliance?

Looking ahead, we anticipate oversight and investigations of PAC providers to continue in the areas described above.

In addition, concerning SNFs, COVID-19 has brought particular scrutiny to SNF compliance, and there has been a push for more regulatory and enforcement activity affecting SNF providers. We anticipate considerable focus will be on whether residents received quality services during the pandemic and SNF responses to COVID-19.

In addition, the government will be focusing on COVID-19-related fraud, including the use of telehealth. The U.S. Department of Justice has a task force specifically focused on this area. Furthermore, OIG is currently auditing the use of and billing for telehealth services provided during the public health emergency, generally[28] and specifically by HHAs under Centers for Medicare & Medicaid Services (CMS) waivers.[29]

PAC providers should ensure their legal and compliance departments review all relationships with referral sources prior to implementing an arrangement.

Compliance departments should focus resources on auditing telehealth services to determine if a PAC provider was potentially noncompliant with the CMS waiver requirements. If noncompliance is identified, the PAC provider should ensure that it returns any payments associated with the noncompliant telehealth service. CT

Endnotes

1. U.S. Department of Health & Human Services, Office of Inspector General, "OIG Special Fraud Alerts: Home Health Fraud, and Fraud and Abuse in the Provision of Medical Supplies to Nursing Facilities," August 10, 1995, https://oig.hhs.gov/documents/special-fraud-alerts/875/081095.html.
2. U.S. Department of Health & Human Services, Office of Inspector General, "Fraud and Abuse in the Provision of Services in Nursing Facilities," Special Fraud Alert, May 1996, https://oig.hhs.gov/documents/special-fraud-alerts/874/SFANursingFacilities.pdf.
3. U.S. Department of Health & Human Services, Office of Inspector General, "Fraud and Abuse in Nursing Home Arrangements with Hospices," Special Fraud Alert, March 1998, https://oig.hhs.gov/documents/special-fraud-alerts/873/hospice.pdf.
4. Robert Holly, "Home Health Providers Have Paid $422M to Settle False Claims Act Cases Since 2012," *Home Health Care News*, July 13, 2021, https://homehealthcarenews.com/2021/07/home-health-providers-have-paid-422m-to-settle-false-claims-act-cases-since-2012/.
5. Suzanne Murrin, *Medicaid Fraud Control Units Fiscal Year 2021 Annual Report*, U.S. Department of Health & Human Services, Office of Inspector General, March 2022, https://oig.hhs.gov/oei/reports/OEI-09-22-00020.pdf.
6. Suzanne Murrin, *Medicaid Fraud Control Units Fiscal Year 2021 Annual Report*.
7. Suzanne Murrin, *Medicaid Fraud Control Units Fiscal Year 2021 Annual Report*.
8. 31 U.S.C. § 3729.
9. 31 U.S.C. § 3729(b)(1).
10. 42 U.S.C. § 1320a–7k(d).
11. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Home Health Provider Agency Compliance Audit: Visiting Nurse Association of Maryland," April 27, 2021, 2, https://oig.hhs.gov/oas/reports/region3/31700009.asp.
12. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Home Health Provider Agency Compliance Audit: Condado Home Care Program, Inc.," August 10, 2020, 4, https://oig.hhs.gov/oas/reports/region2/21701022.asp.
13. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Home Health Provider Agency Compliance Audit: Visiting Nurse Association of Maryland," April 2021, https://oig.hhs.gov/oas/reports/region3/31700009.pdf.
14. U.S. Department of Justice, U.S. Attorney's Office, Northern District of Georgia, "Home health agency to pay $4.2 million to settle False Claims Act allegations," news release, November 22, 2021, https://www.justice.gov/usao-ndga/pr/home-health-agency-pay-42-million-settle-false-claims-act-allegations-0.
15. U.S. Department of Justice, U.S. Attorney's Office, Eastern District of Pennsylvania, "Hospice Care Provider Pays Nearly $6 Million to Resolve False Claims Act Allegations," news release, December 13, 2018, https://www.justice.gov/usao-edpa/pr/hospice-care-provider-pays-nearly-6-million-resolve-false-claims-act-allegations.
16. U.S. Department of Justice, U.S. Attorney's Office, Middle District of Florida, "Hope Hospice Agrees To Pay $3.2 Million To Settle False Claims Act Liability," news release, July 8, 2020, https://www.justice.gov/usao-mdfl/pr/hope-hospice-agrees-pay-32-million-settle-false-claims-act-liability.
17. U.S. Department of Justice, Office of Public Affairs, "Crossroads Hospice Agrees to Pay $5.5 Million to Settle False Claims Act Liability," news release, November 23, 2021, https://www.justice.gov/opa/pr/crossroads-hospice-agrees-pay-55-million-settle-false-claims-act-liability.
18. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Payments of $6.6 Billion to Nonhospice Providers Over 10 Years for Items and Services Provided to Hospice Beneficiaries Suggest the Need for Increased Oversight," data brief, February 2022, https://oig.hhs.gov/oas/reports/region9/92003015.pdf.
19. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Payments of $6.6 Billion to Nonhospice Providers."
20. U.S. Department of Justice, "Diversicare Health Services, Inc. Agrees To Pay $9.5 Million To Resolve False Claims Act Allegations," news release, February 28, 2020, https://www.justice.gov/usao-mdtn/pr/diversicare-health-services-inc-agrees-pay-95-million-resolve-false-claims-act.
21. U.S. Department of Justice, U.S. State Attorney's Office, Southern District of New York, "Manhattan U.S. Attorney Files Suit Against Eleven Skilled Nursing Facilities And Their Management Company, Owner, And A Senior Employee For Fraudulently Billing Medicare For Unnecessary Services," news release, June 2, 2021, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-files-suit-against-eleven-skilled-nursing-facilities-and-their.
22. U.S. Department of Justice, Office of Public Affairs, "SavaSeniorCare LLC Agrees to Pay $11.2 Million to Resolve False Claims Act Allegations," news release, March 21, 2021, https://www.justice.gov/opa/pr/savaseniorcare-llc-agrees-pay-112-million-resolve-false-claims-act-allegations.
23. 42 U.S.C. § 1320a–7b.
24. U.S. Department of Justice, Office of Public Affairs, "United States Files Suit Against California Skilled Nursing Chain and its Owner for Allegedly Paying Illegal Kickbacks to Physicians," news release, June 15, 2021, https://www.justice.gov/opa/pr/united-states-files-suit-against-california-skilled-nursing-chain-and-its-owner-allegedly.
25. U.S. Department of Justice, Office of Public Affairs, "Hospice Administrator Sentenced for Role in Hospice Fraud Scheme," news release, February 19, 2021, https://www.justice.gov/opa/pr/hospice-administrator-sentenced-role-hospice-fraud-scheme.
26. U.S. Department of Justice, Office of Public Affairs, "Home Health Agency Operator BAYADA to Pay $17 Million to Resolve False Claims Act Allegations for Paying Kickback," news release, September 8, 2021, https://www.justice.gov/opa/pr/home-health-agency-operator-bayada-pay-17-million-resolve-false-claims-act-allegations-paying.
27. U.S. Department of Justice, Office of Public Affairs, "Patient Recruiter Pleads Guilty to $870,000 Kickback Scheme," news release, March 11, 2022, https://www.justice.gov/opa/pr/patient-recruiter-pleads-guilty-870000-kickback-scheme.
28. U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Telehealth Services During the COVID-19 Pandemic: Program Integrity Risks," completed September 2, 2022, https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000535.asp.
29. U.S. Department of Health & Human Services, Office of Inspector General, "Audit of Home Health Services Provided as Telehealth During the COVID-19 Public Health Emergency," accessed November 3, 2022, https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000553.asp.

Takeaways

- Post-acute care (PAC) providers have been and continue to be a target of enforcement actions.
- PAC providers' False Claims Act liability risks generally relate to patients or residents not meeting the Medicare eligibility criteria, providing medically unnecessary services, and billing for services not provided.
- PAC providers' relationships with referral sources are closely scrutinized by government agencies as they pose a risk under the Anti-Kickback Statute (AKS).
- Tailored monitoring and auditing of these risk areas and review of referral arrangements under the AKS can mitigate risks.
- The government is focusing on COVID-19-related fraud—especially the use of telehealth—and compliance officers should engage in targeted auditing of telehealth.

SAVE the DATE!

Research Compliance Conference

June 11–13, 2023
Phoenix, AZ

- Research Misconduct
- Compliance Program Effectiveness
- Conflicts of Interest
- Investigations

PLUS:
Receive *complimentary access* to SCCE's *Higher Education Compliance Conference*

Learn how to address emerging risks in research, best practices for dealing with unique compliance challenges, and make valuable industry connections.

Learn more and register
hcca-info.org/2023research

HCCA
Health Care Compliance Association

HOPE FOR THE BEST, EXPECT THE WORST, PLAN TODAY

by François Bodhuin and Gerry Blass

François Bodhuin

(bodhuinf@ihn.org, bit.ly/linked-in-FrancoisBodhuin) is Assistant Vice President and Chief Information Security Officer at Inspira Health, Vineland, NJ.

Gerry Blass

(gerry@complyassistant.com, bit.ly/linked-in-GerryBlass) is CEO at ComplyAssistant, Colts Neck, NJ.

The evolution of the risk of successful cyberattacks has been evident since 2010—when the Affordable Care Act was signed and resulted in a transition from paper to electronic medical records. Healthcare organizations began implementing new electronic medical record applications to comply with meaningful use (MU) requirements. Over the years, MU has introduced new criteria with a heavy focus on interoperability among applications. The combination of MU efforts, merger and acquisition activity, and the pandemic-induced remote workforce have increased healthcare organizations' risk profiles, remaining a prime target for cyberattackers to do what they do best.

There are numerous reasons for the high level of cybersecurity risk in healthcare, such as limited staffing and the technology required to effectively implement controls that reduce risk. These scenarios contribute to higher risk at almost every level of the organization. As a result, we have witnessed successful cyberattacks that have resulted in healthcare organizations experiencing extended downtime for a critical application, their entire network, or somewhere in between.

Furthermore, only 54% of businesses have a documented, community-wide disaster recovery and business continuity (DRBC) plan.[1] Unfortunately, some business executives have taken the "it won't happen to me" approach, and the results can be devastating.

This article is based on more than 60 years of experience in the industry to arm your team with five key questions to consider when implementing a DRBC plan. Now is the time to prepare for the worst.

Question 1: Why do I need a DRBC plan?

The first step in developing a DRBC plan is understanding its purpose. Disaster recovery defines how an organization's IT department will recover from a natural or manufactured disaster, such as restoring necessary applications. Business continuity focuses on the business operations side of DRBC, such as downtime procedures for vital departments and applications.

In today's environment, it is essential for the enterprise emergency management team to understand that cybersafety has a direct line to patient safety. An extensive, successful cyberattack can bring down medical

devices and divert patients to other facilities for necessary treatments such as chemotherapy, dialysis, and intensive care unit (ICU) services. In the past, we would see downtime generally lasting up to 72 hours, whereas today, that number has increased to a month or more. This disruption devastates the healthcare system and the patients who depend on critical care.

It is important to ensure the DRBC plan aligns with an organization's emergency management plan, incident response plan, business impact analysis (BIA), and extended departmental downtime/business continuity procedures.

Question 2: What does extended downtime mean for my business?

We know the systems and technology used at the healthcare-organization level require maintenance. When this occurs, downtime is planned, and procedures are implemented to safeguard advanced notice to staff and minimal disruption to patient care. Unfortunately, what we've seen more often in the past couple of years is incident after incident of "unplanned downtime." Whether it's the result of ransomware or a natural disaster, these situations can be costly and sometimes deadly.

An IBM survey published in July 2021 found that healthcare breaches cost the most of any industry, averaging $9.23 million per incident, which is $2 million more than in 2020.[2] These numbers continue to grow, putting hospitals in a significantly worse place than they've been in years. The bottom line? Whether your system is down for three days or three months, there are detrimental consequences with every passing day. Having a plan won't certify that bad things won't happen, but it *will* confirm that your organization is better equipped to handle them.

Question 3: What does third-party risk have to do with DRBC?

According to the Federal Deposit Insurance Corporation, various types of third-party risk can impact an organization on numerous levels.[3] These include compliance, reputation, strategic, operational, transaction, credit, and country risks. At Inspira Health, a leading charitable nonprofit healthcare organization in southern New Jersey, along with other systems around the country, the chief goal of the chief information security officer (CISO) is to guarantee patient data and lives are protected. While it takes seconds for a patient's protected health information (PHI) and safety to be compromised, it can take weeks or longer to resolve the issue.

Having a DRBC plan in place can help reduce third-party risk and prepare for extended downtime. It is imperative that organizations, regardless of size, assess potential risks as low, medium, or high and plan accordingly. Vendors without access to PHI tend to rank on the low-risk side, and vendors with PHI access are typically in the medium to high-risk category. The average hospital has relationships with vendors of varying risk levels, so conducting periodic BIAs can help establish and maintain the efficacy of your DRBC plan.

Third-party vendors that rank as high risk for your organization must demonstrate that they are working proactively to remedy the underlying issue(s). The process from here is dependent upon both parties. As the entity, you must ensure you're not bringing excess or unnecessary risk into the organization, and the third party must take action to address any potential risk. If these actions can't be achieved in a suitable time frame, it is up to the organization to consider further action.

Whether your system is down for three days or three months, there are detrimental consequences with every passing day.

Question 4: How can I collaborate with other departments in my organization on DRBC?

After you've assessed your major third-party vendors and applications and taken steps to remedy any high-risk threats, the next step is to bring together the proper stakeholders. This team should include leaders from each pertinent department, such as:

- Legal
- Risk management
- Compliance
- IT/security
- Nursing
- Ancillary departments (radiology, laboratory, pharmacy, etc.)
- ICU, emergency department, learning and development
- Finance/human resources/public relations/accounts payable
- Facilities

A tight-knit team helps verify that nothing falls through the

cracks, and each stakeholder can account for their respective department's needs. For example, how long can the finance team keep paying employees if the payroll system is down for an extended time? How does an extensive period of enterprise downtime impact billing, patient care, and interdepartmental communications? These, and more, are considerations in DRBC planning, so it's vital to keep everyone involved throughout the process. Ongoing collaboration and communication will support the overall workflow and necessary procedures to the organization and confirm the continuum of patient care.

While the landscape has changed drastically over the years, one element that hasn't shifted is the reward of being proactive regarding cybersecurity.

An enterprise-wide team will help guarantee that crucial considerations aren't missed or discounted when developing and implementing your plan. It's always enlightening to bring groups together and find that various departments offer vastly different ways to handle a particular issue. While the responsibilities of the team members will vary, some of the valuable roles and tasks include:

- Working collectively to create a BIA
- Assessing the impact of each department's low, medium, and high-risk levels
- Ensuring that high-risk vendors are closely monitored and BA agreements outlining liability are thoroughly assessed
- Identifying the maximum amount of time each department can maintain operations if disaster strikes
- Attending team meetings consistently to check on progress

Question 5: What advice would you give CISOs, information security officers, and other health information managers/professionals?

Start today. Don't delay your efforts to bolster your organization's DRBC plan. While the landscape has changed drastically over the years, one element that hasn't shifted is the reward of being proactive regarding cybersecurity. Though DRBC plans vary across organizations, the essential element is that each organization has a plan so that if a disaster occurs, leaders are prepared to make timely, effective decisions.

The following are some tips we've learned over the years that have contributed to our success.

- **Reduce the risk of a successful cybersecurity attack.** In the fall of 2019, the Office of the National Coordinator for Health Information Technology assigned the U.S. Department of Health & Human Services 405(d) Taskforce to establish the Health Industry Cybersecurity Practices (HICP) in partnership with the National Institute of Standards and Technology and Office for Civil Rights.[4] Collectively, the team identified the five main threats in cybersecurity:
  - Email phishing
  - Ransomware
  - Attacks against connected medical devices
  - Insider, accidental, or intentional data loss
  - Loss or theft of equipment data

Additionally, the team identified 10 controls, or ways to mitigate, the most common threats. HICP and DRBC should go hand in hand because they allow organizations to determine which risks are most relevant and the best ways to alleviate them.

- **Conduct ongoing BIAs.** Invest the time to thoroughly assess your key departments, applications, *and vendors*. It is fundamental to keep your BIA current to account for change management. This activity impacts your DRBC plan and procedures as well as the related plans previously listed. Since a large percentage of successful cyberattacks have originated at the vendor location, implementing a comprehensive, third-party risk management program is crucial. Whether you have one significant application from a vendor, or multiple critical applications (e.g., medical devices vendor), it is important to vet them when they are onboarded and periodically thereafter.
- **Consistency is the DNA of success.** Your DRBC plan and related plans should undergo tabletop testing exercises on a reasonable frequency based on several factors, including organizational size and scope, results of previous tests, and change management (e.g., organizational change and modifications to your network, applications, etc.).

- **Outsource, outsource, outsource.** When there are challenges with internal resources and a need for outside, unbiased subject matter expertise, consider engaging a virtual CISO organization to help fill gaps and provide another set of eyes and ears. The scope of the current risk terrain is significant, which makes outsourcing a potential strategy to enhance your internal resources to reduce the risk of a PHI breach and protect your patients' safety and lives. CT

Endnotes

1. GFiuui45fg, "Only 54% of organizations have a company-wide disaster recovery plan in place," *Cyber Reports*, June 29, 2021, https://cyber-reports.com/2021/06/29/only-54-of-organizations-have-a-company-wide-disaster-recovery-plan-in-place/.
2. "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," *IBM*, July 28, 2021, https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.
3. "VII. Unfair and Deceptive Practices—Third Party Risk," *FDIC Consumer Compliance Examination Manual*, June 2019, https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-4-1.pdf.
4. National Institute of Standards and Technology, Office for Civil Rights, *405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)*, 2019 https://www.nist.gov/system/files/documents/2019/10/16/1-4-hicp-405d-chua-decker-heesters.pdf.

Takeaways

- Understand the current landscape as it pertains to cybersecurity, which includes challenges brought on by the remote workforce and impending threat of extended downtime.
- Know the value of a disaster recovery and business continuity plan, including alignment with an organization's emergency management plan.
- Recognize the various types of third-party risk outlined by the Federal Deposit Insurance Corporation, including compliance, reputation, strategic, operational, transaction, credit, and country risks.
- Discover how to build a high-impact team within your organization, which should include stakeholders from legal, risk management, compliance, IT, nursing, and ancillary departments.
- Learn from your peers. Do not hesitate to copy a methodology if it has been successful and makes sense in your environment.

TAKE YOUR CAREER TO THE NEXT LEVEL

Learn more and get started
hcca-info.org/certification

WHY BECOME CERTIFIED?

Enhance your credibility

Certification validates your compliance knowledge of current trends and regulations within the profession.

Increase your competitive edge

Certification sets you apart in the eyes of current and future employers, demonstrating your higher-level expertise.

Show your commitment to the profession

Compliance Certification Board (CCB)® certification affirms your dedication to the field of compliance, your position, and your organization.

FIVE STEPS TO CERTIFICATION

Gain work experience

Earn and submit CEUs

Apply to take the exam

Schedule your exam

Take the exam

Applying for certification – The application process is easy! Once you have the necessary work experience and CEUs, go to hcca-info.org/apply-exam and fill out the online application form.

CHOOSING YOUR TESTING OPTION

CCB offers a variety of testing options for your convenience:

- Electronic testing at a PSI Testing Center
- A paper and pencil exam at an HCCA conference (per availability)
- A remote proctored exam*: take your test from the comfort and safety of home!

**Offered for all CCB basic certifications, these exams can be scheduled (depending on availability) as soon as two business days after receiving PSI's confirmation, or weeks ahead to accommodate your schedule. Get the details at hcca-info.org/exam-info.*

ALREADY CERTIFIED?

Stay on top of your renewal requirements! – For our comprehensive list of CEU activity options, visit hcca-info.org/how-to-earn-ceus

Live vs. non-live credits – At least 20 of the 40 CEUs required for certification renewal must come from live education. Live CEUs are earned from education presented in real-time with the ability to interact with Q & A. Non-live CEUs are earned when an educational event is not interactive, such as a recorded webinar, authoring an article, self-study, etc.

Need more time to earn CEUs? – As a CCB certification holder, you have a one-month grace period beyond your renewal date to earn and submit CEUs. If additional time is needed beyond the grace period, you may file an extension for up to two additional months to complete the renewal requirements.

CHC™ CERTIFIED IN HEALTHCARE COMPLIANCE

CHPC™ CERTIFIED IN HEALTHCARE PRIVACY COMPLIANCE

CHRC™ CERTIFIED IN HEALTHCARE RESEARCH COMPLIANCE

CCB® COMPLIANCE CERTIFICATION BOARD

Regional Healthcare Compliance Conferences

General and specialty education for every level

These one-day events explore a diverse spectrum of topical compliance issues with educational sessions led by experienced healthcare compliance professionals. Events are either virtual or in-person, depending on location. Attendees will have the opportunity to earn live Compliance Certification Board (CCB)® continuing education units (CEUs).

Get the latest best practices, strategies, and updates in:

Regulatory requirements

Compliance enforcement

Risk management

Maintaining an effective compliance program

Upcoming Events

Each Regional conference features unique sessions and topics—no two events are the same!

January 13, 2023
Charlotte, NC | Virtual

January 20, 2023
Atlanta, GA | In-person

January 27, 2023
Orlando, FL | In-person

February 3, 2023
Portland, OR | In-person

February 10, 2023
Dallas, TX | In-person

February 23, 2023
Alaska | Virtual

February 24, 2023
St. Louis, MO | In-person

March 10, 2023
Washington, DC & Richmond | Virtual

May 19, 2023
New Orleans, LA | Virtual

June 2, 2023
Columbus & Indianapolis | Virtual

June 9, 2023
Orange County, CA | In-person

June 16, 2023
Ann Arbor, MI | In-person

June 23, 2023
New York, NY | In-person

June 23, 2023
Seattle, WA | Virtual

September 8, 2023
Boston, MA | In-Person

September 15, 2023
Minneapolis, MN | In-Person

September 15, 2023
Chicago & Kansas City | Virtual

October 6, 2023
Pittsburgh, PA | In-Person

October 12–13, 2023
Hawaii | In-Person

October 13, 2023
Denver, CO | In-Person

October 20, 2023
Louisville, KY | Virtual

November 3, 2023
Scottsdale, AZ | In-Person

November 17, 2023
Nashville, TN | In-Person

December 1, 2023
San Francisco, CA | In-Person

December 8, 2023
Houston, TX | Virtual

Learn more and register
hcca-info.org/regionals

HCCA®
Health Care Compliance Association

Takeaways

January 2023

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.

How compliance can impact ESG

Nakis Urfi (page 14)

- Environmental, social, and governance (ESG) are nonfinancial factors investors use to measure investments and companies and their overall sustainability impact.
- Organizations are already engaging in many ESG activities, and ESG brings a new lens and framework broadly to these activities.
- Stakeholder expectations and upcoming regulations are driving the movement in the ESG industry.
- There are similarities between running ESG efforts and operating a compliance program.
- Compliance professionals bring great skill sets and capabilities that can lead or help manage ESG activities.

HCCA salary survey reveals a bright compensation picture

Adam Turteltaub (page 20)

- Compensation has generally increased.
- Certification correlates with significantly higher salaries.
- As would be expected, larger organizations generally pay higher than smaller ones.
- Public companies typically offer the highest compensation.
- There are substantial regional variations in compensation.

Identifying and managing risks with third-party relationships

Lisa Taylor, Amy Smith, and Kasie Ray (page 24) **CEU**

- The federal government has emphasized the importance of and increased its scrutiny of third-party management practices within organizations.
- There are various compliance risks when engaging third-party contractors. Ultimately, the risk lies with the contracting entity (not the third-party contractor).
- Buy-in and a commitment to compliance throughout organizational leadership and departments are essential to effectively manage risks with third-party contractors.
- Organizations should have a formal due diligence process to evaluate potential third-party contractors and related risks. Ongoing audits, monitoring plans, risk assessments, and compliance training can be practical tools to mitigate and address risks.
- When terminating third-party contractor agreements, ensure there is a process to confirm that all business information (including protected health information) is returned or destroyed and that all access the third-party contractor had to physical sites or online sites/systems is also ceased.

The importance of a robust third-party compliance program

Amy B. Boring and Stephen P. Cummings (page 30)

- An effective compliance program includes a robust review of third-party vendors.
- A compliance program must look at the entire life cycle of a third-party vendor relationship.
- An appropriate third-party vendor compliance program should include a business need, due diligence, contractual limitations of risks, onboarding, monitoring, and enforcement and a process to conclude the vendor relationship.
- A third-party vendor's business activity and access to confidential information may determine whether a company considers a vendor to be low-risk, medium-risk, or high-risk.
- A company can tailor its compliance program to focus on higher-risk vendors, but it still must ensure appropriate oversight over low- or mid-risk vendors.

Understanding information blocking and the expectations for healthcare organizations

Dawn Morgenstern (page 36) **CEU**

- With few exceptions, healthcare providers, tech vendors, health information exchanges, and health information networks can't prevent electronic personal health information (ePHI) access.
- Information blocking assumes that if HIPAA permits a patient or any other entity or individual to access records, they should be given access without delay, using almost any technology the requester chooses. Those requests do not have to be event-triggered.
- HIPAA-covered entities are expected to comply with HIPAA and the rules of the 21st Century Cures Act.
- There are eight specific exceptions to the rule, with complex implementation standards allowing providers to deny ePHI requests without being considered information blocking.
- Organizations should have well-defined processes to evaluate and review requests, maintain documentation for compliance purposes, and determine how denials are consistently tailored to one or more exceptions.

Reduce OCR enforcement: Get recognized cybersecurity practices in place

Kelly McLendon and Christopher Lyons (page 42)

- Health Industry Cybersecurity Practices (HICP) is a public–private partnership formed as the result of federal law that has produced cybersecurity tools for small, medium, and large organizations.
- The 405(d) cybersecurity practices are drawn from the National Institute of Standards and Technology Cybersecurity Framework.
- Cybersecurity protections for patient information have become so important that the federal government has amended Health Information Technology for Economic and Clinical Health to allow the Office of Civil Rights to favorably view an organization's "recognized security practices."
- Liability is rising across several fronts from civil lawsuits to cyber insurance and regulators requiring increased cyber diligence.
- HICP has identified five threats and 10 recommended cybersecurity practices tailored to organizational size.

Now is the time to prepare for changes to the HIPAA Privacy Rule

Frank Ruelas Jr., Frank Ruelas Sr., and J. Veronica Xu (page 48)

- Currently, the final rule for modifications to HIPAA is expected to be published in March 2023.
- The proposed rules strengthen several key aspects related to an individual's right to access protected health information.
- New requirements that may be finalized include providing individuals with estimates on fees regarding requests for copies of medical records.
- Individuals designated with the responsibility of implementing HIPAA privacy policies may want to consider creating work teams to begin assessing the impact of the proposed changes to the Privacy Rule.
- Covered entities will have 240 days from when the final rule on modifications to the Privacy Rule is published in the *Federal Register* to prepare for enforcement.

Post-acute care providers' fraud risks

Randi Seigel and Krusheeta R. Patel (page 54) **CEU**

- Post-acute care (PAC) providers have been and continue to be a target of enforcement actions.
- PAC providers' False Claims Act liability risks generally relate to patients or residents not meeting the Medicare eligibility criteria, providing medically unnecessary services, and billing for services not provided.
- PAC providers' relationships with referral sources are closely scrutinized by government agencies as they pose a risk under the Anti-Kickback Statute (AKS).
- Tailored monitoring and auditing of these risk areas and review of referral arrangements under the AKS can mitigate risks.
- The government is focusing on COVID-19-related fraud—especially the use of telehealth—and compliance officers should engage in targeted auditing of telehealth.

Hope for the best, expect the worst, plan today

François Bodhuin and Gerry Blass (page 60)

- Understand the current landscape as it pertains to cybersecurity, which includes challenges brought on by the remote workforce and impending threat of extended downtime.
- Know the value of a disaster recovery and business continuity plan, including alignment with an organization's emergency management plan.
- Recognize the various types of third-party risk outlined by the Federal Deposit Insurance Corporation, including compliance, reputation, strategic, operational, transaction, credit, and country risks.
- Discover how to build a high-impact team within your organization, which should include stakeholders from legal, risk management, compliance, IT, nursing, and ancillary departments.
- Learn from your peers. Do not hesitate to copy a methodology if it has been successful and makes sense in your environment.

HCCA upcoming events

JANUARY

January 10
How to Create a Culture of Compliance: Increasing Influence by Building Trust
WEBINAR

January 13
Regional Healthcare Compliance Conference
CHARLOTTE, NC • VIRTUAL

January 18
FCPA Enforcement Update: Lessons Learned for Best Practices
WEBINAR

January 19
SCCE's Sports, Compliance, and Ethics Conference
VIRTUAL

January 20
Regional Healthcare Compliance Conference
ATLANTA, GA • IN-PERSON

January 23–26
Healthcare Basic Compliance Academy
ORLANDO, FL • IN-PERSON

January 23–26
Healthcare Privacy Compliance Academy
ORLANDO, FL • IN-PERSON

January 27
Regional Healthcare Compliance Conference
ORLANDO, FL • IN-PERSON

Jan 31–Feb 2
Managed Care Compliance Conference
VIRTUAL

FEBRUARY

February 3
Regional Healthcare Compliance Conference
PORTLAND, OR • IN-PERSON

February 6–9
Healthcare Compliance Essentials Workshop
VIRTUAL

February 8
SCCE's Bootstrapping Ethics
WEBINAR

February 10
Regional Healthcare Compliance Conference
DALLAS, TX • IN-PERSON

February 23
Regional Healthcare Compliance Conference
ALASKA • VIRTUAL

February 24
Regional Healthcare Compliance Conference
ST. LOUIS, MO • IN-PERSON

2023 We continue to add events and dates to our schedule. Please check the website for details.

Managed Care Compliance Conference
January 31–February 2 · VIRTUAL (CT)

27th Annual Compliance Institute
April 23–26 · Anaheim, CA · IN-PERSON
April 24–26 · VIRTUAL (PT)

Research Compliance Conference
June 11–13 · Phoenix, AZ · IN-PERSON

Clinical Practice Compliance Conference
October 10–11 · VIRTUAL (CT)

Healthcare Compliance Essentials Workshops
February 6–9 · VIRTUAL (CT)
May 15–18 · VIRTUAL (CT)
September 18–21 · VIRTUAL (CT)
December 4–7 · VIRTUAL (CT)

Webinars
Stay up-to-date on timely topics specific to the healthcare industry and earn Compliance Certification Board (CCB)® CEUs without travel. Visit hcca-info.org/webinars to see our latest offerings.

Healthcare Basic Compliance Academies
January 23–26 · Orlando, FL · IN-PERSON
March 6–9 · Phoenix, AZ · IN-PERSON
April 3–6 · Nashville, TN · IN-PERSON
May 8–11 · Chicago, IL · IN-PERSON
July 24–27 · New Orleans, LA · IN-PERSON
August 21–24 · Washington, DC · IN-PERSON
December 11–14 · Orlando, FL · IN-PERSON

Healthcare Privacy Compliance Academies
January 23–26 · Orlando, FL · IN-PERSON
March 6–9 · Phoenix, AZ · IN-PERSON
May 8–11 · Chicago, IL · IN-PERSON
August 21–24 · Washington, DC · IN-PERSON
December 11–14 · Orlando, FL · IN-PERSON

Healthcare Research Compliance Academies
March 6–9 · Phoenix, AZ · IN-PERSON
December 11–14 · Orlando, FL · IN-PERSON

Regional Healthcare Compliance Conferences
January 13 · Charlotte, NC · VIRTUAL
January 20 · Atlanta, GA · IN-PERSON
January 27 · Orlando, FL · IN-PERSON
February 3 · Portland, OR · IN-PERSON
February 10 · Dallas, TX · IN-PERSON
February 23 · Alaska · VIRTUAL
February 24 · St. Louis, MO · IN-PERSON
March 10 · Washington, DC & Richmond, VA · VIRTUAL
May 19 · New Orleans, LA · VIRTUAL
June 2 · Columbus & Indianapolis · VIRTUAL
June 9 · Orange County, CA · IN-PERSON
June 16 · Ann Arbor, MI · IN-PERSON
June 23 · New York, NY · IN-PERSON
June 23 · Seattle, WA · VIRTUAL
September 8 · Boston, MA · IN-PERSON
September 15 · Minneapolis, MN · IN-PERSON
September 15 · Chicago & Kansas City · VIRTUAL
October 6 · Pittsburgh, PA · IN-PERSON
October 12–13 · Hawaii · IN-PERSON
October 13 · Denver, CO · IN-PERSON
October 20 · Louisville, KY · VIRTUAL
November 3 · Scottsdale, AZ · IN-PERSON
November 17 · Nashville, TN · IN-PERSON
December 1 · San Francisco, CA · IN-PERSON
December 8 · Houston, TX · VIRTUAL

Event dates are subject to change.
Visit **hcca-info.org/events** to learn more.

HCCA Health Care Compliance Association

HCCA COMPLIANCE 101

Explore the fundamentals of healthcare compliance

Newly updated and in its fifth edition, *HCCA Compliance 101* is an overview of compliance programs and a compliance officer's role. Perfect for new practitioners, board members, or staff education, this book features guidance and insight on:

- Benefits and administration of a compliance program that follows the seven essential elements
- Government guidance and laws
- Patient privacy and security
- Risk assessment, monitoring, and auditing
- Program assessment and measuring effectiveness

Now in its fifth edition!

HCCA Compliance 101 has been updated with new insights and tips on how to build an effective compliance program. All new chapters focus on risk assessment, investigations, government oversight, and more, as well as new sample policies, forms, and further resources to explore.

About the authors

Debbie Troklus and Sheryl Vacca have extensive compliance and risk management experience in both corporate and healthcare settings. Troklus and Vacca sit on the SCCE® & HCCA® Board of Directors and serve as key faculty members at SCCE & HCCA Academies. Darrell W. Contreras is a licensed attorney who has worked for more than 25 years in healthcare compliance, is a frequent lecturer on compliance and privacy topics, and is faculty member for HCCA's Compliance and Privacy Academies.

Learn more
hcca-info.org/compliance101

HCCA®
Health Care Compliance Association

Virtual Healthcare Compliance Essentials Workshop

Essential knowledge for your compliance career

Whether you're new to compliance or have been practicing for a while and need a refresher, attending an HCCA Healthcare Compliance Essentials Workshop is for you!

In this four-day virtual workshop, industry leaders will guide you through the core elements of a healthcare compliance program and get you caught up on the latest strategies and best practices for you to bring back to your organization.

Workshop topics include:

- Introduction to compliance & ethics programs
- Due diligence in delegation of authority
- Investigations
- Key skills necessary for compliance professionals
- Standards & procedures
- Communication & training
- Response to wrongdoing
- Governance, oversights, and authority
- Incentives & enforcement
- Program improvement
- Risk assessment
- Monitoring, auditing, & reporting systems
- HIPAA, Stark Law, Anti-Kickback Statute, and False Claims Act

Upcoming 2023 Workshops

February 6–9
May 15–18
September 18–21
December 4–7

All workshops are held in Central Time (CT)

Learn more and register
hcca-info.org/essentials

HCCA
Health Care Compliance Association