March–April 2022

# Journal of Health Care Compliance


What DOJ Cares About in 2022: Reading the Signs

Ransomware Attacks on Healthcare Providers—What You Need to Know

The No Surprises Act—Not in Compliance According to Surprised Providers

Compliance Considerations for Entities Providing Hybrid Clinical Trial Services

What's in Your Pocketbook? The Value and Necessity of Compliance Program Effectiveness Reviews

High Impact, Unique Risks—What Compliance Professionals Need to Know About the 340B Drug Discount Program

Wolters Kluwer

10041440-0320

Journal of
# Health Care Compliance

Volume 24, Number 2
March–April 2022

## Columns



## Features



## For the Record

Journal of
# Health Care Compliance

**Editor-in-chief**
Roy Snell

**Managing Editor**
Jeanine Mazzorana

**Cover Design**
Patrick Gallagher

**Interior Design**
Jason Wommack



## Editorial Board





**Journal of Health Care Compliance** (ISSN: 15208) is published bimonthly by Wolters Kluwer.

**Customer Service:** For customer service call 1-800-234-1660.

**Business and circulation:** Distribution Center, Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704.

**Permission requests:** For permission on how to obtain permission to reprint content, please send an e-mail to http://www.wklawbusiness.com/footer-pages/permissions or FAX 847 267-2516.

**Reprints:** For customized article reprint, please contact Wright's Media at 1-877-652-5295 or go the the Wright's Media Web site at www.wrightsmedia.com

*Roy Snell*

# What's New in Compliance—Chaos and Opportunity Will Be Plentiful

We have many recent and upcoming changes that will significantly impact compliance professionals and compliance programs. The impact of the COVID pandemic alone will be multifaceted. I have heard many stories about how the compliance officer was pulled in early and often to help with the organization's pandemic management efforts. I personally think that the bigger the problem, the more likely leadership will pull in the compliance officer. Most compliance officers are skilled at handing stress. Leadership needs calm people more than they have ever needed them in the past. There are also some very specific changes that will impact the compliance department such as telemedicine compliance. Telemedicine was plodding along and then exploded as a result of the pandemic. Rapid change increases compliance risks.

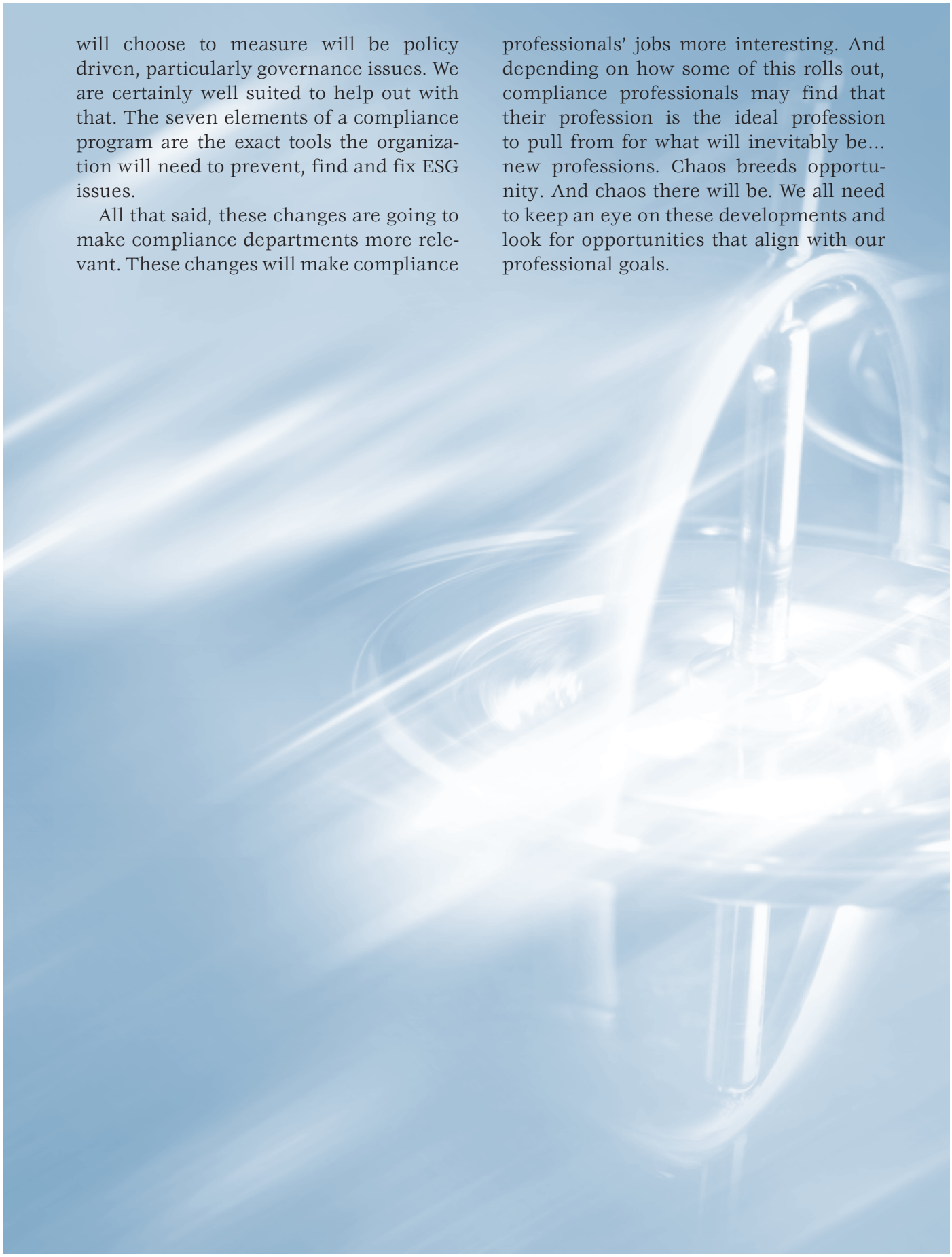
We also have the ongoing evolution of artificial intelligence and its impact on compliance. If you think trying to get humans to stop breaking the law and behave ethically is difficult, try working with computer software that has a mind of its own. The impact of AI on organizational culture may be significant. Of particular interest will be the privacy issues. If AI software misuses personal data there will be material problems with employees and customers. People are very concerned about AI privacy issues and there will be many potential problems. However, what may be a bigger problem is the lack of understanding of AI. Many people believe AI is a mythical, mystical and uncontrollable beast. The assumption by many is that AI is evil. Some people will assume the worst. AI creates fear, uncertainty, and doubt. None of that is good for the compliance professional who, in part, is hired to keep the peace. We have to comprehensively investigate and respond to allegations of wrongdoing regardless of their validity.

Maybe the biggest change coming up for compliance professionals will be the implementation of Environmental, Social, and Governance programs. Anyone who thinks non-profit healthcare organizations will be exempt from implementing ESG will be sorely disappointed. The implementation of ESG programs are going to go well beyond publicly traded companies. Compliance is well versed to help out with existing ESG related laws, particularly with regard to the environment and social issues. Our work with the HR department on social issues may increase significantly. Much of ESG will go beyond the rule of law. Many of the ESG metrics your organization

**Roy Snell** is the ESG and Sustainability Officer for Osprey ESG Software. Roy is the co-founder of the Health Care Compliance Association and the Society of Corporate Compliance. He is the author of Integrity Works and The Accidental Compliance Professional.

will choose to measure will be policy driven, particularly governance issues. We are certainly well suited to help out with that. The seven elements of a compliance program are the exact tools the organization will need to prevent, find and fix ESG issues.

All that said, these changes are going to make compliance departments more relevant. These changes will make compliance professionals' jobs more interesting. And depending on how some of this rolls out, compliance professionals may find that their profession is the ideal profession to pull from for what will inevitably be… new professions. Chaos breeds opportunity. And chaos there will be. We all need to keep an eye on these developments and look for opportunities that align with our professional goals.



# What DOJ Cares About in 2022: Reading the Signs

**Jaime L.M. Jones / Brenna E. Jenny**

**Jaime L.M. Jones** is global co-leader of the Healthcare practice at Sidley Austin LLP and serves on the firm's COVID-19 task force. She represents leading institutional health-care providers and life sciences companies in civil and criminal government enforcement matters and FCA litigation.

**Brenna E. Jenny** is a partner in the Healthcare practice at Sidley Austin LLP and previously served as Principal Deputy General Counsel of HHS and the Chief Legal Officer of CMS. She represents clients in the healthcare industry in government enforcement actions, internal investigations, and compliance reviews.

The Department of Justice (DOJ) has long prioritized enforcement actions in the healthcare industry, and the pandemic only intensified DOJ's focus. Whenever DOJ announces a significant False Claims Act (FCA) settlement, intervention, or litigation victory, it issues a carefully crafted press release describing the alleged misconduct at issue. These press releases provide important clues about the theories of liability that are of particular interest to DOJ and offer a roadmap for in-house legal and compliance professionals of how to tailor internal compliance controls to stay apace with DOJ's evolving interests. Below are the enforcement areas of priority for the industry gleaned from DOJ's 2021 healthcare enforcement press releases.

## Kickbacks Remain a Priority

Across the healthcare industry, alleged violations of the Anti-Kickback Statute (AKS) were a significant driver of settlements last year. This has been a consistent trend across the last two decades, and we expect this to continue in 2022. The AKS's incredibly broad reach means that it sweeps in a range of business relationships and transactions that would be lawful in many other industries. These settlements serve as a reminder that where arrangements cannot be safe harbored, healthcare companies must carefully evaluate risk and implement compliance oversight to ensure they do not involve unlawful inducements.

## Independent Contractor Relationships

Recently, DOJ has paid particular attention to independent contractor relationships in the healthcare and life sciences space. In March 2021, DOJ issued a press release announcing that the Fourth Circuit Court of Appeals had affirmed a DOJ victory in an FCA case predicated on commission-based arrangements with contracted sales organizations found to have violated the AKS.[1] The clinical laboratory in that case offered commission-based compensation to an independent contractor, BlueWave, which also reimbursed its own downstream sales representatives on a commission basis. DOJ argued that both

arrangements violated the AKS, because independent contractors could not take advantage of the employee safe harbor and furthermore the arrangements did not satisfy all of the requirements of the personal services safe harbor, including that compensation for the services performed not take into account the volume or value of referrals.

The case was dismissed by some as an unremarkable AKS enforcement action in light of the allegations that the underlying conduct resulted in medically unnecessary lab tests and the commission payments at issue were very high. But the remarkable aspect of the case emerged from the press release, in which DOJ chose to focus not on these factors, but rather broadly stated that the arrangements at issue "constituted 'remuneration' intended to induce BlueWave's sales representatives to sell as many blood tests as possible," and furthermore declared that the AKS "prohibited BlueWave from paying its salespeople for recommending the tests." Nonemployee contract salesforces are standard in some sectors of the healthcare and life sciences industries, and broadly equating them with unlawful remuneration to recommend products is inconsistent with the more nuanced approach the Department of Health and Human Services Office of Inspector General (HHS-OIG) has taken with respect to AKS enforcement.

DOJ continued to enter into settlements over the past year involving arrangements premised on independent contractor relationships, characterizing the misconduct at issue as violating the AKS because "the amount of the kickback was based either on a percentage or fixed amount of Medicare's reimbursement for each test"[2] or "illegal remuneration [was offered] ... in the form of volume-based commissions paid to independent contractor recruiters."[3] Atmospheric factors such as medical necessity continue to factor into DOJ's calculation of when to pursue an AKS case based on independent contractor relationships, but it is far from clear that DOJ would not pursue independent contractor compensation-based cases absent these aggravating facts. Thus, DOJ's recent focus on this space increases the importance of ensuring that where sales-based compensation relationships cannot be safe harbored, organizations need to understand and be prepared to accept the attendant enforcement risks. It also becomes critically important to implement appropriate compliance guardrails to prevent compensation arrangements from appearing to induce medically unnecessary sales, the promotion of products in ways that are false or misleading, or other conduct that heightens any healthcare organization's overall enforcement risk.

## Equity Transactions

Mergers and acquisitions among healthcare providers have reached a frenetic pace in recent years, and DOJ has expressed clear interest in gauging whether equity-based healthcare transactions—both those occurring as part of changes of ownership as well as those that do not—implicate the AKS.

In December 2021, DOJ announced a settlement with a partially physician-owned hospital, which resolved allegations that the hospital repurchased shares from retiring physicians and "impermissibly took into account the volume or value of certain physicians' referrals when it (1) selected the physicians to whom the shares would be resold and (2) determined the number of shares each physician would receive."[4] This settlement comes on the heels of other settlements in recent years involving allegations that remuneration in the form of equity was offered in exchange for referrals. For example, DOJ entered into settlements to resolve allegations that: a hospital purchased a physician practice and ambulatory surgery center at a price above fair market value, based on expected volume of referrals,[5] and a hospital provided remuneration to a physician group in the form of equity

buyback provisions that exceeded fair market value.[6]

Equity grants are common and appropriate aspects of transactions and may reflect a variety of factors completely independent of referrals, such as legacy ownership structures. Nonetheless, taken together these settlements highlight that equity grants, including those as part of physician roll-ups, can implicate healthcare fraud and abuse laws and trigger government enforcement scrutiny if not structured appropriately.

### Joint Ventures

DOJ and HHS-OIG have historically approached joint ventures with some skepticism, concerned that such arrangements are merely efforts to strategically enter into business relationships that mask the exchange of remuneration for referrals. Of course, healthcare joint ventures play important roles in driving efficiency, coordination, and quality of care, in turn decreasing costs to the system and helping to achieve other HHS priorities. As HHS-OIG recently noted in a negative advisory opinion regarding a proposed joint venture arrangement, however, these business relationships are suspect if seemingly "designed to permit [an entity] to do indirectly what it cannot do directly: pay the JV Partner a share of the profits from the JV Partner's referrals."[7]

A recent district court opinion relating to a co-management model—a common form of joint venture—highlights the ongoing risk. In 2020, DOJ belatedly sought to intervene in the case, following an earlier declination.[8] Citing new findings from additional data analytics work, which allowed DOJ to analyze "Medicare claims data and match[] the documents detailing various forms of remuneration with claims data to identify FCA violations," the government argued the requisite good cause standard to intervene after declining was met.[9] The district court denied the government's motion but, late last year, it also denied the defendants' motion to dismiss. At issue in the case is a co-management model deployed by a cataract surgery center, in which the ophthalmologist who performs a cataract surgery receives 80% of the fee for the surgery, while the referring optometrist who does the follow-up care receives 20%. Defendants argued that this is a lawful, referral-based, co-management business model, and simply providing the opportunity to earn a co-management fee is not remuneration. In contrast, the relators' view of the arrangement is that through the mere opportunity to earn a fee, "optometrists are lured into sending their patients to Defendants' eye surgeons," in violation of the AKS. The district court agreed that these allegations met the expansive "one purpose" test, under which a payment can violate the AKS so long as one purpose is to induce referrals.

Providers considering strategic joint ventures should carefully consider relevant HHS-OIG guidance and take advantage of safe harbor protection where feasible, including the new value-based care safe harbors.

## Billing and Coding

Alleged misconduct relating to billing and coding was the largest driver of settlements among healthcare providers in 2021. Providers can expect billing and coding to continue to attract significant DOJ scrutiny, with a particular focus on the temporary billing flexibilities authorized by HHS during the pandemic and the ever-expanding Medicare Advantage (MA) program.

### Pandemic Regulatory Flexibilities

To bring relief to providers hit hard by the COVID-19 pandemic, beginning in March 2020 HHS began offering a variety of temporary billing flexibilities, generally tethered to the pendency of the public health emergency. These flexibilities took multiple forms, including announcements of enforcement discretion policies and the use of HHS' waiver authority under Social

Security Act Section 1135, which allows HHS to modify or waive certain statutory and regulatory requirements. It was through this waiver authority that HHS was able to significantly alter longstanding billing rules, such as by dramatically expanding the scope of Medicare-payable telehealth services.

On May 17, 2021, DOJ announced the formation of a COVID-19 Fraud Enforcement Task Force "to marshal the resources of the Department of Justice in partnership with agencies across government to enhance enforcement efforts against COVID-19 related fraud."[10] In press releases throughout 2021, DOJ reiterated its commitment to prioritizing fraud related to the pandemic. For example, less than two weeks after the announcement of the Task Force, DOJ heralded a string of recent criminal charges against defendants "alleged to have engaged in various health care fraud schemes designed to exploit the COVID-19 pandemic."[11]

So far, DOJ's efforts to combat COVID-19–related fraud have manifested primarily as criminal charges against individual bad actors engaged in conduct such as selling "snake oil" or taking pandemic relief funds to purchase sports cars. However, there are reasons to believe that DOJ will expand beyond these run-of-the-mill fraud cases to pursue more nuanced theories of civil liability under the FCA. First, DOJ has made clear that as a matter of policy, pandemic fraud is a priority. When announcing highlights from its fiscal year 2021 fraud recoveries, DOJ emphasized how it is has been working "closely with various Inspector Generals and other agency stakeholders to identify, monitor and investigate the misuse of critical pandemic relief monies."[12] And the COVID-19 task force mirrors the highly successful, and still active, Prescription Interdiction & Litigation (PIL) Task Force that DOJ announced in 2018, which has resulted in a number of criminal and civil charges stemming from the opioid abuse crisis.[13] Second, it is highly unlikely that fraud in this space is limited to criminal matters. If anything, the complexity of the shifting billing rules makes it more difficult to establish criminal scienter, leaving a civil—or administrative—resolution as the more appropriate option for resolving billing errors. More nuanced theories relating to abuse of pandemic billing flexibilities can be expected to take longer to develop than blatant fraud, particularly because many of these cases may arise under seal as *qui tam* suits filed by whistleblowers under the FCA. HHS-OIG has a number of items on its work plan relating to pandemic billing practices, especially with respect to telehealth, and the expected publication of these reports in 2022 can be expected to generate further interest from the whistleblower's bar. In the meantime, providers should ensure that legal and compliance functions have a line of sight on the policies and practices for how billing flexibilities have been implemented. Data-driven compliance monitoring can help provide early visibility into outlier billing areas warranting further evaluation.

## MA Retrospective Chart Reviews

HHS has been slow to exercise significant administrative oversight of the MA program, including by providing few concrete rules regarding expected documentation to support the diagnosis codes that control MA plan, and often downstream provider, reimbursement. Over the past decade, as the MA program has continued its significant growth, DOJ has stepped into the gap and announced through enforcement actions its own expectations for medical record documentation. DOJ entered into one settlement last year with an MA provider for $90 million[14] and intervened in two other cases.[15] Litigation over alleged upcoding in the MA program remains ongoing in these and other cases, and in DOJ's press release announcing its fiscal year 2021 fraud recoveries, MA fraud was described second in the list of

highlights, behind only abuses related to opioids.

DOJ's enforcement activity has been particularly challenging for MA participants not only because DOJ has frequently announced new interpretations of regulatory obligations for the first time in enforcement actions, but also because its expectations have evolved. Over the past few years, DOJ has focused on the use of retrospective chart reviews to abstract diagnosis codes from patient charts. One type of review that has drawn DOJ's ire in particular are so-called "one-way" chart reviews. According to DOJ, these reviews are problematic because they are designed to allow MA plans and providers to identify and submit previously unsubmitted diagnosis codes, but they do not test the sufficiency of documentation for codes already submitted. DOJ views these chart reviews as a violation of the obligation to report and return identified overpayments.

But more recently, in the two cases in which DOJ intervened last year, DOJ raised broader concerns about codes added through chart reviews, even when they are not "one-way." For example, as explained in a press release announcing DOJ's intervention in multiple *qui tams* against a particular MA plan, DOJ explained that MAOs may "submit diagnoses to CMS only for conditions that required or affected patient care, treatment or management during an in-person encounter in the service year. In order to increase its Medicare reimbursements, [the MA plan] allegedly pressured its physicians to create addenda to medical records after the patient encounter, often months or over a year later, to add risk-adjusting diagnoses that patients did not actually have and/or were not actually considered or addressed during the encounter, in violation of Medicare requirements."[16] DOJ appears skeptical that a treating practitioner could have sufficiently documented a condition affecting patient care, treatment, or management while contemporaneous coding practices did not result in the submission of an associated diagnosis code.

In light of DOJ's newly articulated concerns over the extent to which retrospectively abstracted codes are lawful because they may not have affected patient care, treatment, or management at the time of the encounter, MA plans and providers should evaluate the scope of their retrospective chart reviews and consider whether modifications are necessary to reduce risk in light of DOJ's evolving expectations.

## Intersection Between Competition and Fraud and Abuse Concerns

DOJ has begun to comingle concerns relating to anticompetitive conduct and fraud and abuse, and this conceptual blending is likely to appear in other cases this year, raising the threat that conduct alleged to be anticompetitive may not pique the Federal Trade Commission's interest but could instead attract DOJ scrutiny from a healthcare fraud and abuse perspective. In October 2021, DOJ announced settlements with a trio of generic drug companies "to resolve alleged violations of the False Claims Act arising from conspiracies to fix the price of various generic drugs[, which] allegedly resulted in higher drug prices for federal health care programs and beneficiaries."[17] In particular, the "three companies paid and received compensation prohibited by the Anti-Kickback Statute through arrangements on price, supply and allocation of customers with other pharmaceutical manufacturers for certain generic drugs manufactured by the companies."[18] Thus, although framed in part as AKS violations, the proposition that anticompetitive conduct can "artificially inflate prices" and result in false claims may be raised by DOJ as a standalone theory separate from kickbacks. This is particularly true in light of the Biden administration's stated intentions to promote competition in the healthcare industry.[19] DOJ's statements also highlight the risk of joint ventures, discussed above,

especially between potential competitors in a marketplace.

## Looking Ahead

DOJ's recently released fiscal year 2021 FCA statistics[20] revealed that 90% of recoveries last year were from the healthcare industry, demonstrating that once again, this industry received disproportionate scrutiny. While 2022 will surely bring new areas of enforcement, we do not expect the healthcare industry more broadly, or any of the specific areas discussed above, to become less important to DOJ. Healthcare companies should ensure their compliance organizations are appropriately resourced to meet the challenges.

### Endnotes

1. Press Release, DOJ, Fourth Circuit Court of Appeals Affirms $114 Million Judgment Against 3 Defendants Found Liable of Defrauding Medicare and Tricare (Mar. 8, 2021), *https://www.justice.gov/usao-sc/pr/fourth-circuit-court-appeals-affirms-114-million-judgment-against-3-defendants-found*.
2. Press Release, DOJ, AutoGenomics, Inc. Agrees to Pay Over $2.5 Million for Allegedly Paying Kickbacks (Jan. 11, 2021), *https://www.justice.gov/usao-wdwi/pr/autogenomics-inc-agrees-pay-over-25-million-allegedly-paying-kickbacks*.
3. Press Release, DOJ, Seven Texas Doctors and a Hospital CEO Agree to Pay over $1.1 Million to Settle Kickback Allegations (Jan. 20, 2022), *https://www.justice.gov/usao-edtx/pr/seven-texas-doctors-and-hospital-ceo-agree-pay-over-11-million-settle-kickback*.
4. Press Release, DOJ, Flower Mound Hospital to Pay $18.2 Million to Settle Federal and State False Claims Act Allegations Arising from Improper Inducements to Referring Physicians (Dec. 2, 2021), *https://www.justice.gov/opa/pr/flower-mound-hospital-pay-182-million-settle-federal-and-state-false-claims-act-allegations*.
5. Press Release, DOJ, Prime Healthcare Services and Two Doctors Agree to Pay $37.5 Million to Settle Allegations of Kickbacks, Billing for a Suspended Doctor, and False Claims for Implantable Medical Hardware (July 19, 2021), *https://www.justice.gov/opa/pr/prime-healthcare-services-and-two-doctors-agree-pay-375-million-settle-allegations-kickbacks*.
6. Press Release, DOJ, Oklahoma City Hospital, Management Company, And Physician Group To Pay $72.3 Million To Settle Federal And State False Claims Act Allegations Arising From Improper Payments To Referring Physicians (July 8, 2020); *https://www.justice.gov/opa/pr/oklahoma-city-hospital-management-company-and-physician-group-pay-723-million-settle-federal*.
7. HHS-OIG, Adv. Op. No. 21-18 (Nov. 17, 2021), *https://oig.hhs.gov/compliance/advisory-opinions/21-18/*.
8. *United States ex rel. Odom v. Southeast Eye Specialists*, No. 17-cv-689 (M.D. Tenn. Apr. 7, 2017).
9. United States' Memorandum of Law Supporting Its Motion to Intervene, Add Two Defendants, and Stay the Suit for 90 Days, Dkt. #288 at 4–5, *United States ex rel. Odom v. Southeast Eye Specialists*, No. 17-cv-689 (M.D. Tenn. Feb. 10, 2020).
10. Press Release, DOJ, Attorney General Announces Task Force to Combat COVID-19 Fraud (May 17, 2021), *https://www.justice.gov/opa/pr/attorney-general-announces-task-force-combat-covid-19-fraud*.
11. Press Release, DOJ, DOJ Announces Coordinated Law Enforcement Action to Combat Health Care Fraud Related to COVID-19 (May 26, 2021), *https://www.justice.gov/opa/pr/doj-announces-coordinated-law-enforcement-action-combat-health-care-fraud-related-covid-19*.
12. Press Release, DOJ, Justice Department's False Claims Act Settlements and Judgments Exceed $5.6 Billion in Fiscal Year 2021 (Feb. 1, 2022), *https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year*.
13. Press Release, DOJ, Attorney General Sessions Announces New Prescription Interdiction & Litigation Task Force (Feb. 27, 2018), *https://www.justice.gov/opa/pr/attorney-general-sessions-announces-new-prescription-interdiction-litigation-task-force*.
14. Press Release, DOJ, Sutter Health and Affiliates to Pay $90 Million to Settle False Claims Act Allegations of Mischarging the Medicare Advantage Program (Aug. 30, 2021), *https://www.justice.gov/opa/pr/sutter-health-and-affiliates-pay-90-million-settle-false-claims-act-allegations-mischarging*.
15. Press Release, DOJ, United States Intervenes and Files Complaint in False Claims Act Suit Against Health Insurer for Submitting Unsupported Diagnoses to the Medicare Advantage Program (Sept. 14, 2021), *https://www.justice.gov/opa/pr/united-states-intervenes-and-files-complaint-false-claims-act-suit-against-health-insurer*; Press Release, DOJ, Government Intervenes in False Claims Act Lawsuits Against Kaiser Permanente Affiliates for Submitting Inaccurate Diagnosis Codes to the Medicare Advantage Program (July 30, 2021), *https://www.justice.gov/opa/pr/government-intervenes-false-claims-act-lawsuits-against-kaiser-permanente-affiliates*.
16. Press Release, DOJ, Government Intervenes in False Claims Act Lawsuits Against Kaiser Permanente Affiliates for Submitting Inaccurate Diagnosis Codes to the Medicare Advantage Program (July 30, 2021), *https://www.justice.gov/opa/pr/government-intervenes-false-claims-act-lawsuits-against-kaiser-permanente-affiliates*.

Continued on page 69

# Ransomware Attacks on Healthcare Providers—What You Need to Know

**Phyllis Sumner / Rob Keenan**

As cyberattacks increase generally, ransomware attacks have gained particular prominence in today's headlines. And if things weren't already bad enough, the COVID-19 pandemic has added the vulnerabilities of a remote workforce, and supplied tempting content for fraudulent communications, often impersonating company executives or government authorities, used to dupe unwary recipients into furnishing information system access to cyber criminals. Unfortunately, healthcare providers are among the favorite targets of ransomware gangs.

This article will survey the sobering statistics of cyberattacks, including ransomware, in the healthcare industry; the shifting tactics of ransomware attackers; key incident response issues; HIPAA breach analysis steps; proactive planning; cyber insurance considerations; and tips for preserving the attorney–client privilege.

**Phyllis Sumner** is a partner with King & Spalding and the firm's Chief Privacy Officer. Ms. Sumner leads King & Spalding's Data, Privacy and Security (DPS) Practice Group.

**Rob Keenan** is a partner with King & Spalding and Chair of the firm's HIPAA Business Associate Committee.

## The Numbers

Breaches caused by malicious cyberattacks continue to escalate. No industry segment is impacted more than healthcare, which suffered nearly 25% of all data breaches in 2020, almost 10% more than the second-ranked technology sector.[1]

For the institutional victim, data breaches are difficult, time-consuming—and expensive. Affected entities must incur substantial costs to identify and contain an incident; analyze data and make required notifications; address the concerns of impacted individuals and regulators; and deal with business disruption from downtime and reputational impact. On top of that daunting list, these victims of ransomware attacks often face regulatory investigations and enforcement actions as well as class actions.

Breaches are particularly costly for healthcare providers. In 2020, the average total cost of a data breach across all industry segments was $3.9 million, which

actually was down slightly from 2019.[2] The healthcare industry, however, topped the 18 industry segment categories with an average data breach cost of over $7 million, a 10% increase from 2019.[3]

Ransomware recently replaced business email compromise (BEC) as the leading type of malicious cyberattack. Healthcare providers are particularly attractive to ransomware gangs because of the potentially drastic consequences of business interruption. It may not be surprising, then, that nearly half of all healthcare industry breaches are attributable to ransomware attacks.[4] Adding insult to injury, ransomware attacks result in more costly data breaches when compared to other types of malicious attacks.[5]

## Shifting Tactics of Ransomware Attackers

Ransomware is a type of malicious software, or malware that blocks access to data in a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. Historically, ransomware attackers focused almost exclusively on encryption, and were not otherwise interested in the underlying data. Increasingly, however, ransomware attackers have upped the ante by exfiltrating data and threatening to publish it on the dark Web on so-called "shaming sites," sometimes even auctioning stolen data to the highest bidder. Although a relatively new tactic that first gained momentum only as recently as early 2020, exfiltration now is commonly coupled with encryption to pose a potent ransomware double threat.[6] In some instances, these attackers forgo the ransomware and demand a ransom based only on stolen data.

In addition, ransomware attackers have evolved from undisciplined criminal gangs into slick business-type enterprises, adopting attributes of legitimate businesses, like franchising ransomware tools to other criminal actors for a percentage of the take, known as ransomware-as-a-service or RaaS. Attackers often will furnish detailed penetration reports describing how the victim's vulnerabilities were exploited. In a perverse adaptation of a marketing department, ransomware attackers may contact the victim's employees and business partners to escalate pressure on the ransom payment decision.

For those who agree to pay, some ransomware attackers offer "call centers" with representatives standing by to furnish decryption instructions or file trees of stolen data. Ransomware attackers most often require payment in Bitcoin, but increasingly are seeking payment in less traceable cryptocurrencies like Monero, and may even offer a discount for use of a less traceable crypto. All of these techniques have leveraged the prevalence and success of ransomware enterprises.

## Incident Response Challenges

### Threat Actor Engagement

Ransomware victims initially may be eager to contact the threat actor to identify the ransom price and find out what information was stolen. Victims should pause, however, to carefully consider whether threat actor engagement will reduce or increase risk. At a minimum, victims should thoroughly diligence the threat actor before engaging. When engagement is warranted, experienced threat actor negotiators are available to help professionalize and diligence the engagement. Further, while some ransom gangs pride themselves on acting professionally, others are abusive and harassing in their tactics, which may make it more difficult to manage and evaluate the risk. Even for those purporting to act like professionals, companies should be wary of the risk of engaging with criminals who are not accountable or identifiable.

### Law Enforcement Engagement

Other questions to consider are whether and when to engage with law enforcement. While some organizations can be

reticent about quickly reaching out to law enforcement in the early stages of an incident, a variety of law enforcement agencies can be very helpful by providing threat intelligence about the ransom gangs. Information such as the characteristics and modus operandi of ransomware attackers can be enormously helpful to assist a company perform diligence before engaging or potentially paying a threat actor. For example, FBI field offices gather detailed threat intelligence that can be invaluable to incident response decision making.

Companies should define a law enforcement engagement process in advance, including who will make the contact, and to whom the contact will be made. Ideally, the company or outside counsel will have an established law enforcement agency contact identified in advance as part of the company's incident response plan. If not, the company or counsel should contact the appropriate law enforcement agency's cyber division instead of making a cold call to a general agency number.

### To Pay or Not to Pay?

Despite the risks of paying criminal actors, more than half of companies subject to a ransomware attack pay ransom. Whether or not to pay ransom can be an extremely difficult decision. Victims may feel that they have no other option, particularly if both primary and backup systems are encrypted, and sensitive data has been exfiltrated. Although they can be much higher, ransom payments on average are less than $150,000, which explains why companies often are willing and even eager to pay. Still, companies should carefully consider the pros and cons of paying ransom.

Payment risks are considerable. Ransomware attackers promise to fully de-encrypt systems, destroy stolen data, and go away, but those promises too often are not kept or are only partially kept. Companies that pay ransom get tagged as a payer, and repeat extortion is common. Payments to entities on the U.S. Office of Foreign Assets Control (OFAC) sanctions list could subject the victim to civil and possibly even criminal sanctions. Accordingly, companies should pay a ransom only as a last resort after all other reasonable options have been explored and exhausted.

## Breach Analysis

### HIPAA

Healthcare providers will need to evaluate a ransomware event under the HIPAA breach notification rule (Breach Notification Rule).[7] Under HIPAA, "breach" means the acquisition, access, use, or disclosure of protected health information or PHI in a manner not permitted by the HIPAA privacy rule (Privacy Rule) that compromises the security or privacy of the PHI.[8] The term "compromises" is not defined.

When PHI has been acquired, accessed, used, or disclosed in a manner not permitted by the privacy rule, a breach is presumed unless the covered entity (or business associate) demonstrates that there is a "low probability" that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.[9]

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) has published ransomware guidance.[10] According to the OCR: "When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession

or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[11] This statement, taken in isolation, has confused some readers. As OCR subsequently notes, a breach does not occur simply by virtue of ransomware encryption, but only occurs if the entity determines that the information has been compromised based on a risk assessment.[12]

There are two distinct steps to the HIPAA breach analysis: (i) was the information acquired, accessed, used, or disclosed in violation of the Privacy Rule; and (ii) if so, was the information compromised. If there is no prohibited acquisition, access, use, or disclosure, there is no breach, and no need to do a risk assessment.

One court decision may impact the view that PHI is "acquired" in violation of the Privacy Rule when the entity has lost control of the information, such as through encryption in a ransomware attack. In *University of Texas M.D. Anderson Cancer Center v. U.S. Department of Health and Human Services*,[13] ("*M.D. Anderson*"), the U.S. Court of Appeals for the Fifth Circuit considered whether the loss of an unencrypted laptop and thumb drives containing the PHI of 35,000 individuals resulted in a "disclosure" of the PHI. An administrative law judge (ALJ) previously had determined that M.D. Anderson's loss of control of the ePHI on the laptop and thumb drives had resulted in a disclosure. The Fifth Circuit disagreed and concluded that disclosure required an affirmative act to release information and not merely the loss of control.[14]

As a practical matter, the HIPAA breach assessment of a ransomware event will turn on the forensic analysis of the event and whether PHI was exfiltrated or viewed. If it was not, a HIPAA covered entity or business associate may determine that the PHI was not acquired, accessed, used, or disclosed in violation of the Privacy Rule, in which case no breach has occurred. In the alternative, the entity may conclude that even if the information was acquired under the "loss of control" theory, there was no compromise based on a risk assessment.

The quality and detail of the forensic analysis and its evidentiary underpinnings will be critical to this analysis. Ransomware attackers often infiltrate a company's electronic systems without detection for weeks or months, and increasingly employ techniques designed to wipe its fingerprints before it is even detected. Conclusions that exfiltration or access did not occur may be difficult to support and defend in the absence of affirmative forensic evidence to that effect. The existence of such evidence always falls on a continuum between no evidence and conclusive evidence, and covered entities and business associates should diligently pressure test the forensic analysis and conclusions in this regard.

### State Law

HIPAA does not preempt state breach notification laws, which typically are applied based on the state of an individual's residence, without regard to the location of the affected entity. Most state breach notification laws defer to HIPAA in some way. Some state laws do not apply to entities subject to HIPAA.[15] Others do not apply to the extent that an entity makes breach notifications required by HIPAA.[16] Still others may provide that state individual notice requirements are met when HIPAA individual notification requirements are satisfied, but such laws may impose additional requirements, such as notification to the state attorney general.[17]

## Breach Notification

In the event that a data breach has occurred and no exceptions apply,[18] notifications will be required. The Breach Notification Rule provides that individuals be notified without unreasonable delay and in no case later than 60 calendar days after "discovery" of the breach.[19] For breaches

involving 500 or more individuals, notification to OCR follows the same timeline.[20] For breaches involving fewer than 500 individuals, reports to OCR are required within 60 days after the end of the calendar year in which the breach occurred.[21] For breaches involving more than 500 individuals, reporting to prominent media outlets may be required.[22]

"Discovery" means the first day on which a breach is known to the covered entity or, by exercising reasonable diligence would have been known.[23] Identifying the HIPAA discovery date is complicated, because the OCR has interpreted it to relate back to the first date that a potential breach has been identified, even if it has not yet been confirmed that a breach occurred. According to the OCR: "Under this rule, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule."[24] As noted above, however, the actual regulatory definition defines discovery to occur when a *breach* is known or reasonably should have been known, not when the underlying event first is known.

The OCR interpretation is understandable, because the OCR wants to avoid open-ended breach investigations not rigorously conducted in good faith in a timely manner. Nevertheless, ransomware investigations are time consuming and complicated. Ransomware attackers intentionally obfuscate the facts.

Covered entities and business associates should, when possible, conclude investigations and make required notifications within 60 days of first identifying the underlying event, to mitigate risk in relation to OCR's interpretation. But, this is not always reasonable or even possible. Premature notifications do not benefit anyone. It is critical to conduct a thorough investigation, with all deliberate speed. When that occurs, notifications made more than 60 days from first learning of the event may be reasonable and defensible consistent with the literal terms of the Breach Notification Rule.

## Insurance Considerations

It is important to coordinate thoughtfully up front with the cyber carrier (and possibly also the broker) in order to preserve all available coverage for the costs of a data security incident. In addition, there may be other types of insurance not specifically denominated as cyber coverage that could apply to a ransomware incident, such as business interruption or general crimes insurance. The company should carefully review coverage terms to ensure that initial notifications are adequate and timely. Companies are well advised to get a common interest agreement in place at the outset to maximize privilege protections. This applies not only to the carrier but also to the broker if the broker is involved in privileged communications.

Although the carrier may request updates in writing, we recommend getting the carrier's agreement to furnish oral updates. The facts in any cyberattack always evolve, and it's preferable for that reason if possible to commit relatively less to writing as the situation changes. Note other specific coverage requirements, including advance approval requirements for third-party vendors. Some cyber policies require selection of vendors from predetermined panels. If there is potential coverage for a ransom payment, it is important to identify applicable requirements, including to perform threat actor diligence and obtain ransom payment approval before negotiating a payment.

## Incident Response Planning

Comprehensive, advance incident response planning and testing are invaluable. Many companies have sophisticated IT and security incident response plans and playbooks but have not developed, integrated, and tested enterprise-wide plans. The legal

team should develop an incident response playbook that includes privilege protocols set in advance to streamline and facilitate education of the business on how to establish and preserve the attorney–client privilege. Companies also should develop a communications playbook that establishes a centralized clearinghouse to promote consistency of communications, both to internal and external stakeholders. Inconsistent communications can create considerable risk and have a long shelf life.

The best incident response plans identify specific third-party vendors in advance, with specific contact information, including outside counsel, forensic investigator, threat actor negotiator, public relations firm, payment facilitator, and logistics firm. Each vendor should be approved by the cyber carrier and engaged in advance.

Then—practice, practice, practice. We recommend at least annual tabletop exercises that extend throughout the enterprise to include not only IT, legal, and communications teams but also executives and even the Board. It also can be very helpful to include some of the vendors with whom you might find yourself shoulder to shoulder during a significant incident.

Not surprisingly, effective advance incident response planning will significantly reduce the costs associated with a data breach. On average, businesses with comprehensive and tested incident response plans reduced data breach costs by $2 million.[25]

In addition to measurable cost savings, advance planning will help moderate the psychological impact to the enterprise when a data breach occurs. Especially when it's your first rodeo, companies can waste valuable time, energy, and resources working through shock and denial, and trying to stand up and execute a plan from scratch, when company departments actually may be inclined to circle their respective wagons internally if they have not planned and practiced working together. Having a specific and familiar incident response process will add some semblance of a routine to help a company navigate through the inevitable turmoil and disruption of a major data security incident.

## Attorney–Client Privilege Considerations

Data security incident investigations often reveal potential issues with the company's privacy and security infrastructure that require advice from counsel regarding legal compliance, and that will generate communications that should be protected by the attorney–client privilege. Recent judicial decisions, however, have put some pressure on the applicability of the attorney–client privilege in the context of data security incident investigations.[26] Because of this, it is important to maintain rigorous hygiene regarding both the form and substance of privileged engagements and communications in order to maximize preservation of the privilege.

To be privileged, the incident investigation must be conducted under the direction of counsel for the purpose of giving legal advice to the company. Third-party vendors conducting privileged activities should be engaged by counsel—not by the business—using a so-called "Kovel" letter to make clear that the vendor is being engaged to work under the direction of counsel to enable counsel to render legal advice to the company, and that all work product and deliverables should be labeled and treated as privileged and confidential. Similar direction should be given within the company, as applicable.[27]

No detail is too small. For example, it is preferable that vendors working under the privilege actually be paid by the legal department for privileged services instead of being paid by another department. Often, vendors engaged in advance as part of the incident response plan may have

Continued on page 69

# The No Surprises Act—Not in Compliance According to Surprised Providers

**Danielle C. Gordet / Kirk S. Davis**

**Danielle C. Gordet** is an associate with Akerman and focuses her practice on healthcare, including healthcare compliance, conflicts of interest, scope of practice issues, physician contracting, and regulations. Her ability to identify, investigate, and resolve complex issues in collaboration with healthcare administrators allows her to provide them with effective counsel in developing policies and procedures which reduce the risk of inappropriate conduct and prevent non-compliance. She provides expertise on federal and state healthcare statutory and regulatory issues, including adherence to theStark Law, the Anti-Kickback Statute, and licensure compliance. In addition, Danielle assists manufacturers of U.S. Food and Drug Administration (FDA) regulated products in obtaining necessary FDA clearances for their devices.

**Kirk S. Davis** is a partner with Akerman. An accomplished litigator, Mr. Davis represents hospitals and health systems in complex regulatory compliance issues and disputes with a focus on medical malpractice and peer review hearings.

Kirk has decades of experience in the peer review process and has been involved in all aspects of hearings, from prosecuting physicians to defending medical staff and serving as a hearing officer. He helps hospitals comply with federal and state laws by recommending peer review best practices and procedures. In addition to his work on medical malpractice matters, Kirk handles disputes between physicians in private practices and effectively resolves contentious medical practice dissolution through alternative dispute resolution.

New billing protections recently went into effect that have the goal of providing greater protections for patients against surprise medical bills. The Departments of Health and Human Services (HHS), Labor, and Treasury (collectively, the "Departments") and the Office of Personnel Management issued an interim final rule (Interim Rule) with comment period on September 30, 2021,[1] that implements provisions of the No Surprises Act (the "Act").[2] The majority of the provisions in the Interim Rule became effective January 1, 2022. Several lawsuits have been filed, with the consistent theme that healthcare providers are concerned the new provisions unfairly protect group health plans and health insurance issuers (collectively, "Plans") to the detriment of patients and out-of-network physicians and facilities (collectively, "Out-of-Network Providers").

Among other things, the Interim Rule:

- Requires certain providers, including physicians, providers of air ambulance services, and facilities to offer good faith estimates of expected charges for items and services to uninsured or self-pay individuals (collectively, "self-pay individuals"). The estimate also must include any item or service that is reasonably expected to be provided *in conjunction* with the scheduled item or service and any item or service reasonably expected to be provided by another health care provider or facility. HHS understands it may take time for providers "to develop systems and processes for receiving and providing the required information" to or from providers in other facilities. Therefore, from January 1, 2022, through December 31, 2022, HHS will defer enforcement in situations where a good faith estimate is provided to a self-pay individual, but does ***not*** include expected charges from other providers or facilities.
- Protects self-pay individuals from being billed an amount ***substantially in excess*** of the good faith estimate they received. "Substantially in excess" is

defined as an amount that is at least $400 more than the provider's total amount of expected charges listed on the good faith estimate. Patients will be able to initiate a patient-provider dispute resolution process in situations where the provider does not comply with providing a "good faith estimate."

- Creates an Independent Dispute Resolution (IDR) process for Plans and Out-of-Network Providers. The IDR process allows the parties to determine the out-of-network rate for items and services, including certain emergency, nonemergency, and air ambulance services.

Of the above provisions, the addition of the IDR process, described in further detail below, has caused the most criticism.

## Federal IDR Process

A federal IDR process, similar to arbitration, was established to allow Plans and Out-of-Network Providers to resolve disputes regarding out-of-network rates.

If a claim is made for certain out-of-network items or services and the parties cannot agree on the amount to be paid, either party has 30 business days to open negotiations with the other party as to the out-of-network cost. If they cannot agree on the amount to be paid, they must exhaust the 30-day negotiation period before initiating the IDR process. Once the negotiation period is exhausted, a party wishing to begin the IDR process must do so within four business days of the end of the negotiation period—the ***IDR initiation date***. The initiation of the IDR process is not mandatory; however, once the process is initiated by one of the parties, both parties must comply with the requirements. A party that fails to comply with the IDR process opens the risk of the other party's offer being selected, as will be further described below.

The IDR initiation date occurs when the initiating party submits a Notice of IDR Initiation to the other party and to the Departments within that four-business day window. The notice should include the initiating party's preferred certified IDR entity, if applicable. If the initiating party selects a certified IDR entity, the non-initiating party can accept or object to the use of that entity. The parties must come to an agreement on the certified IDR entity within three business days of the IDR initiation date. As alluded to earlier, a party who fails to comply with the IDR process once it is initiated will only harm themselves: "A lack of response from the non-initiating party **within 3 business days** will be deemed to be acceptance of the initiating party's preferred certified IDR entity."[3]

If the parties cannot jointly select a certified IDR entity, the Departments will select one for them within six days of the IDR initiation date. The Interim Rule does not specify if this decision is made by one of the Departments or jointly by all of the Departments. The certified IDR entity selected will be one that charges a fee within the ranges permitted by the Departments, which varies based on the type of determination being made, but, in general, ranges from $200 to $670.[4] "If there are insufficient certified IDR entities available that charge a fee within the allowed range, the Departments will randomly select a certified IDR entity that has approval to charge a fee outside of that range."[5] A certified IDR entity is only permitted to charge a fee that is outside of the range if it has written approval from the Departments. To be granted approval to charge a higher fee, the certified IDR entity must submit a written proposal to the Department that includes: (1) the alternative flat fee it believes is appropriate; (2) a description of the circumstances that require the alternative flat fee; and (3) a description of how the alternative flat fee will be used to mitigate such circumstances.

Within three business days of its selection, the certified IDR entity must attest

that it does not have a conflict with either party and determine that the IDR process is applicable.

No later than 10 days after the certified IDR entity is selected, the parties must each submit to the certified IDR entity an offer for a payment amount for the item or service being disputed. "At the time at which offers from both parties should have been submitted, if one party has not submitted an offer, the certified IDR entity will accept the other party's offer."[6] At this time, each party must "pay the certified IDR entity fee, which the certified IDR entity will hold in a trust or an escrow account, and the administrative fee when submitting its offer."

The certified IDR entity uses the information submitted by the parties to determine the appropriate out-of-network amount. Until recently, the ***certified IDR entity was required to begin with the presumption that the qualifying payment amount (QPA) is the appropriate amount***. In general, the QPA is the Plan's median contracted rate for the same or similar service in the specific geographic area. This presumption is the basis of the controversy as the Out-of-Network Providers deem a Plan's median contracted rate to be an unfair starting point for negotiations. Below we discuss how Out-of-Network Providers successfully argued against this and what it means going forward.

The IDR certified entity shall make a payment determination no later than 30 business days after the date that the certified IDR entity is selected. Any payment due must be paid to the applicable party within 30 business days of the payment determination.

In this article we provide an annotated chart, similar to the one CMS provided, to assist the parties in complying with the IDR process.[7,8]

The certified IDR entity's decision is binding unless there is evidence of fraud or evidence of intentional misrepresentation of material facts presented to the certified IDR entity regarding the claim. Specifically, the decision by the certified IDR entity is not subject to judicial review unless:

- The award was procured by corruption, fraud, or undue means;
- There was evident partiality or corruption in the arbitrator;
- The arbitrator was guilty of misconduct in refusing to postpone the hearing, upon sufficient cause shown, or in refusing to hear evidence pertinent and material to the controversy; or of any other misbehavior by which the rights of any party have been prejudiced; or
- The arbitrator exceeded his or her powers, or so imperfectly executed them that a mutual, final, and definite award upon the subject matter submitted was not made.

## Compliance with Applicable State Law Is Required

When a state law determines the total amount payable under a plan for emergency services or to Out-of-Network Providers at in-network facilities, the state law will apply, rather than the federal IDR process. In addition, new state laws in response to the Interim Rule are anticipated in the future. "The Departments anticipate that some states with their own IDR process may want to change their laws or adopt new laws in response to these interim final rules. The Departments anticipate that these states will incur a small incremental cost when making changes to their laws."

The remainder of this article, however, addresses only the federal IDR process.

## Uproar Against the Interim Rule and a Big Win for Out-of-Network Providers

A number of Out-of-Network Providers and others who support them are pushing

| IDR Actions | Timeline |
|---|---|
| ***Initiation of Open Negotiation Period***<br>Either party may initiate the 30-business-day open negotiation period. The parties must exhaust the 30 business-day open negotiation period before initiating the IDR process. | 30 business days, starting on the day of initial payment or notice of denial of payment |
| ***IDR Initiation***<br>Either party may initiate the IDR process following failed open negotiation. | Within 4 business days, starting the business day after the open negotiation period ends (the day the Notice of IDR Initiation is provided to the other party is the **IDR initiation date**) |
| ***Selection of Certified IDR Entity***<br>The parties must mutually agree on the certified IDR entity.<br>If the parties cannot agree on a certified IDR entity, they must notify the Departments to request a certified IDR entity be selected for them. | The parties must mutually agree on the certified IDR entity within 3 business days after the IDR initiation date<br>If applicable, the Departments will randomly select a certified IDR entity no later than 6 business days after the IDR initiation date |
| ***Certified IDR Entity Attestation of No Conflicts of Interest***<br>The certified IDR entity must submit an attestation that it does not have a conflict of interest and determine that the Federal IDR Process is applicable. | Within 3 business days after selection |
| ***Submission of Offers and Payment of Certified IDR Entity Fee***<br>The parties must submit payment offers and additional information to the certified IDR entity. The parties must also pay the certified IDR entity fee, which the certified IDR entity will hold in a trust or an escrow account. | No later than 10 business days after the selection of the certified IDR entity |
| ***Selection of Offer***<br>Payment determination made by the certified IDR entity. The certified IDR entity notifies the parties and the Departments. | 30 business days after the date of certified IDR entity selection |
| ***Payments Between Parties of Determination Amount & Refund of the Certified IDR Entity Fee***<br>Any amount due from one party to the other party must be paid, and the certified IDR entity must refund the prevailing party's certified IDR entity fee. | 30 business days after the payment determination |

back against the Interim Rule, arguing that it does not comply with intent of the Act. Most recently, they succeeded in doing so when the Texas Medical Association, a trade association representing more than 55,000 physicians, and Dr. Adam Corley filed and won a lawsuit against the Departments. The plaintiffs successfully argued that the Interim Rule unfairly protects Plans to the detriment of patients and Out-of-Network Providers.[9]

The United States District Court for the Eastern District of Texas held that the portions of the Interim Rule relating to the creation of the IDR process must be set aside. Specifically, the court invalidated the portion of the IDR process that hampered Out-of-Network Providers' efforts

to negotiate payment rates. The remaining provisions of the Interim Rule and the Act, however, are still in effect and may be used by the certified IDR entity when determining the framework for resolving payment disputes.

### The Interim Rule Inappropriately Conflicts with the Act

The court agreed with the Texas plaintiffs – portions of the Interim Rule conflict with the Act. The Administrative Procedure Act (APA) requires that the conflicting sections of the Interim Rule must be set aside.[10]

The plaintiffs argued that the Interim Rule creates a rebuttable presumption in favor of the offer closest to the QPA, which is inappropriate. The Act provides for *a number of factors* that should be considered by the certified IDR entity when it is determining the appropriate out-of-network rate to be paid. Despite the Act's requirement to consider a number of factors, the court held that the Interim Rule instead created a rebuttable presumption to first select a rate closest to the QPA. That is, unless credible information clearly demonstrated that the QPA is materially different from the appropriate out-of-network rate.

### The Departments Failed to Provide Adequate Time for Notice and Comment

The court's second basis for setting aside disputed portions of the Interim Rule was that the Departments' bypassed the notice and comment period requirements of the APA.

The APA requires that agencies publish a notice of proposed rule making and give interested persons an opportunity to "participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation."[11] While there are exceptions to this, no exception existed here. Instead, the court noted that if the plaintiffs had been provided appropriate time for notice and comment, they could have submitted to the Departments the specific reasons why they believe the Interim Rule is inconsistent with the Act, how they are impacted, and how the Interim Rule could more accurately track the statutory text.

## Factors the Certified IDR Entity Considers When Deciding if the QPA Is Appropriate

In response to the Texas court's decision, the certified IDR entity is now required to consider all of the statutory factors provided by the Act, instead of automatically giving the greatest weight to the QPA. We have outlined the factors that the certified IDR entity must now consider when deciding whether the QPA is the appropriate out-of-network amount.

The certified IDR entity will consider the following credible information when determining the appropriate out-of-network rate for the item or service:

- ***Experience and Training:*** Did the QPA fail to consider the experience or level of training of the Out-of-Network Provider, which was necessary to provide the items or services to the patient?
- ***The Plan's Market Share:*** Does the Plan have the majority of the market share in the geographic region where the items or services were provided? For example, a Plan that has the majority of the market share in a geographic region may establish that the QPA is unreasonably low, as Plans with a large market share could drive down rates.
- ***Patient Acuity or Complexity of Furnishing the Service is an Outlier:*** Did the intensity of care exceed what is typical for the particular service code or modifier, thereby helping to establish that the QPA does not adequately take the case's complexity into account?

- ***Teaching Status, Case Mix, and Scope of Services:*** Does the out-of-network facility have capabilities that were critical to the delivery of the item or service? For example, a hospital's trauma level certification may be considered when the item or service involves trauma care that could not be performed at a lower-level hospital, but only if the QPA does not already account for this factor.
- ***Good-Faith Efforts by Out-of-Network Provider:*** Did the Out-of-Network Provider make good-faith efforts to enter into a network agreement with the Plan? If the parties had a network agreement in the past, the certified IDR entity may also consider what the contracted rates between the parties were when the network agreement was in place.
- ***Additional Information:*** Was any additional information submitted by the Out-of-Network Provider, to the extent the information is credible and relates to the offer submitted by either party?

## More Surprises to Come

On February 28, 2022, HHS addressed how the decision would impact implementation of the Act by issuing a memorandum for consumers.[12] HHS reassured consumers that the Texas ruling does not impact other portions of the Act. For example, "consumers continue to be protected from surprise bills for out-of-network emergency services, out-of-network air ambulance services, and certain out-of-network services received at in-network facilities." HHS also addressed providers and Plans, noting that the Departments are taking steps to conform to the Texas decision by taking the following immediate actions:

- Withdrawing guidance documents that are based on, or that refer to, the invalidated portions of the Interim Rule. Once these documents are updated to conform with the court's order, the Departments will repost them.
- Providing training on the revised guidance regarding the IDR process.
- Opening the IDR Portal for submissions. If the open negotiation period has expired, the Departments will allow submission of a notice of initiation of the IDR process within 15 business days following the opening of the IDR Portal.

To be compliant, Plans and Out-of-Network Providers must ensure the necessary measures have been put in place to adhere to the IDR process, including its timing requirements. Although a portion of the Interim Rule was struck down, the remainder of the IDR process is in effect. Out-of-Network Providers and Plans have been required to comply as of January 1, 2022. On September 30, 2021, the Departments opened the application process for entities to become certified as IDR entities. Applications are still being accepted on a rolling basis. A list of those certified IDR entities which have successfully been certified as such, is available on the CMS website.[13] As of March 8, 2022, there are only ten certified IDR entities, including, but not limited to, utilization management companies and peer review organizations.

There likely will be continued push-back against the Interim Rule in the days and months to come. There are also a number of other pending cases against the Departments. For example, a lawsuit that the American Hospital Association, the American Medical Association, and other co-plaintiffs filed against the Departments in the United States District Court for the District of Columbia. No order has been issued on that case; however, the Texas decision has and will cause an impact.

### Endnotes

1. 86 Fed. Reg. 55980 (Oct. 7, 2021), Requirements Related to Surprise Billing; Part II, available here: *https://www.govinfo.gov/content/pkg/FR-2021-10-07/pdf/2021-21441.pdf.*
2. 42 U.S.C. 300gg-111.

Continued on page 70

# Compliance Considerations for Entities Providing Hybrid Clinical Trial Services

**Kyle Y. Faget**

## Introduction

COVID-19 disrupted a plethora of clinical trials. With social distancing measures firmly in place and many institutions only seeing patients for urgent needs, clinical trials were stalled indefinitely, which means investigative treatments were also stalled. COVID-19 also spurred, and in many ways forced, unprecedented use of telehealth. Not surprisingly, institutions began implementing telehealth into clinical trials. Since the beginning of COVID-19, clinical trials have been leveraging the powerful tool of telehealth, which promises to effectively blow the doors off of the geographic barriers that have long plagued clinical trial enrollment. A somewhat newly minted business model has emerged—hybrid clinical trial services. Here, an entity supports a clinical trial by providing clinicians that can carry out elements of a protocol *via* telehealth and elements of a clinical trial *via* in home services. The study subject may never have to enter an investigator's brick and mortar office. Entrants into this burgeoning field and industry sponsors are inquiring about how to structure this offering compliantly and how to utilize telehealth compliantly.

**Kyle Y. Faget** is a partner with Foley & Lardner, LLP and Co-Chair of the firm's Health Care Practice Group.

## Clinical Research as the Practice of Medicine

Companies interested in providing hybrid clinical trial services have a threshold issue to resolve; is carrying out the clinical aspects of a clinical trial the practice of medicine? Some argue that simply carrying out the clinical aspects of a predetermined protocol is not the practice of medicine. Others point to the clinical care required in the context of an adverse event, which requires independent clinical judgement on the part of the clinician.

There exists evidence under state law that performance of clinical research constitutes the practice of medicine. Under Tex. Admin. Code § 177.1(2)(emphasis added), Texas defines actively engaged in the practice of medicine as follows:

> The physician on a full-time basis is engaged in diagnosing, treating or offering to treat any mental or physical disease or disorder or any physical deformity or injury or performing such actions with respect to individual patients for compensation and *shall include clinical medical research, the practice of clinical investigative medicine*, the supervision and training of medical students or residents in a teaching facility or program approved by the Liaison Committee on Medical Education of the American Medical Association, the American Osteopathic Association or the Accreditation Council for Graduate Medical Education, and professional managerial, administrative, or supervisory activities related to the practice of medicine or the delivery of health care services. The term 'full-time basis,' for purposes of this section, shall mean at least 20 hours per week for 40 weeks duration during a given year.

Texas, therefore, explicitly includes "*clinical medical research*" in its definition of the practice of medicine, as well as "professional managerial, administrative, or supervisory activities related to the practice of medicine or the delivery of health care services." Not all states will necessarily agree with Texas, but the fact that there exists states such as Texas that explicitly include clinical medical research in the definition of engaging in the practice of medicine means that entities entering the clinical research support services space must consider this issue when thinking about building a scalable corporate structure.

## Corporate Practice of Medicine

If, in a given state, practicing clinical research constitutes the practice of medicine, the corporate practice of medicine doctrine must be considered. Under this doctrine, a number of states prohibit the practice of licensed professions by general corporations, and, instead, require that licensed professions operate *via* a professional corporation or association. In the context of clinical trials, the corporate practice of medicine doctrine prohibits an entity from delivering medical services or employing physicians if the entity is owned by lay persons (*i.e.*, non-physicians).

The theory underlying the corporate practice of medicine is that clinicians, by virtue of, for example, having taken the Hippocratic Oath, must make decisions based on what is in the best interest of a patient, whereas officers and employees of general corporations must make decisions based on profit maximizing principles. The underlying incentives for non-licensed professionals could result in decision-making that is not in the best interest of a patient. This is a state law issue, and some states have no prohibition on the corporate practice of medicine. Nonetheless, many states have enacted corporate practice laws and regulations that prohibit this scenario from ever occurring by limiting ownership in professional corporations or associations to licensed clinicians.

For example, through statutes, regulations, court opinions, and medical board opinions, the law in Texas prohibits general corporations from practicing medicine, or employing or contracting with physicians to practice through such entities, because such entities cannot hold a medical license.[1] Under Tex. Admin. Code § 177.17(a), Texas law "generally prohibits corporations, entities or non-physicians from practicing medicine." Tex. Occ. Code § 155.001 restricts any person from practicing medicine unless the person is a licensed physician. Further, Tex. Occ. Code § 165.156 states that a "person, partnership, trust, association, or corporation commits an offense if the person, partnership, trust, association, or corporation, through the use of any letters,

words, or terms affixed on stationery or on advertisements, or in any other manner," indicates that such person, corporation, or other entity is entitled to practice medicine if such person or entity is not licensed to do so.[2]

Arizona case law generally prohibits corporations and other non-professional business entities from employing health care practitioners to render professional services.[3] Arizona Title 32, ch. 13, Art. 1 defines a "Doctor of Medicine" as a "natural person holding a license, registration or permit to practice medicine pursuant to this chapter."[4]

Colorado prohibits the practice of medicine by non-professional corporations and prohibit licensed professionals from accepting employment from unlicensed person. Colo. Rev. Stat. Ann. § 12-36-134(7) provides, "(a) Corporations shall not practice medicine. Nothing in this section shall be construed to abrogate a cause of action against a professional corporation for its independent acts of negligence. (b) Employment of a physician in accordance with section 25-3-103.7, C.R.S., [addressing hospitals] shall not be considered the corporate practice of medicine.". There is additional guidance on this issue in the context of a dental practice. Colorado defines it as unprofessional conduct to practice medicine as the partner, agent, or employee of, or in joint venture with, any person who does not hold a license to practice within the state.[5]

## Friendly-PC Model

Entities with lay ownership interested in entering into the clinical trial business must consider compliance with the corporate practice of medicine where such laws exist. Many such entities opt to adopt a friendly-PC structure, which is a professional corporation (PC) organized for the purpose of conducting a medical practice in affiliation with a management services organization (MSO). This structure is designed to comply with state corporate practice of medicine restrictions that would prevent a non-professional or a business corporation from practicing medicine or related professions. This is an attractive option for entities founded by non-physicians or that plan to seek external capital funding resulting in lay ownership (*i.e.*, ownership by non-physicians). The affiliation between the MSO and the friendly PC is achieved through a hand-in-hand close working relationship between the MSO and the PC owner, as well as a series of contractual agreements, the MSO's provision of management services, and sometimes start-up financing for the PC. The overall arrangement is intended to allow the MSO to handle the management side of the PC's operations without infringing on the professional judgment of the PC or the medical practice of its physicians and the PC owner.

If structured and *operationalized* properly, the friendly PC model is intended to withstand allegations that the management company or its owners are violating the prohibition on corporate practice of medicine. Notwithstanding the foregoing, the friendly PC model is not "bulletproof" and there remains an irreducible risk it may be challenged as disallowed, particularly in states with a history of strong enforcement of the prohibition on the corporate practice of medicine. Despite the regulatory risk, companies use a friendly PC structure, and the structure generally remains the best-available model for achieving the business goals of the lay owners of a management company. The regulatory risks have historically been accepted by lay owners and investors, many of whom use some form of friendly PC model in states with corporate practice of medicine restrictions.

## PC Owner

In addition to corporate practice considerations, a number of states require that a professional corporation owner be licensed to practice in the state in which the entity is operating. For example,

Utah law provides, "Except as provided in Subsection (1)(b), a person may not be an officer, director, or shareholder of a professional corporation unless that person is: (i) an individual licensed to render the same specific professional services as those for which the corporation is organized; or (ii) qualified to be an officer, director, or shareholder under the applicable licensing act for the profession for which the corporation is organized." "A professional corporation may issue the shares of its capital stock and a shareholder may voluntarily transfer shares of capital stock in a professional corporation only to: (a) persons who are duly licensed to render the same specific professional services as those for which the corporation was organized; or (b) persons other than those meeting the requirements of Subsection (1)(a) to the extent and in the proportions allowed by the applicable licensing act for the profession for which the corporation is organized."[6] "Professional service" means "the personal service rendered by: (a) a physician, surgeon, or doctor of medicine holding a license under Title 58, Chapter 67, Utah Medical Practice Act, and any subsequent laws regulating the practice of medicine."[7]

Similarly, Colorado law provides, "Except as specified in subparagraph (II) of this paragraph (d), all shareholders of the corporation are persons licensed by the board to practice medicine in the state of Colorado who at all times own their shares in their own right; except that one or more persons licensed by the board as a physician assistant may be a shareholder of the corporation as long as the physician shareholders maintain majority ownership of the corporation."[8]

The result of these state imposed licensure requirements is that entities interested in forming a friendly-PC must also identify and contract with a physician owner of the applicable professional corporation or association that is appropriately licensed in each such state.

## Investigator Licensure

In addition to the friendly-PC owner requiring licensure in a number of states, the clinicians providing clinical services generally must be licensed in the state in which the study subject is located. This is an important principle in the context of hybrid clinical trials. While most appreciate that a clinician providing in home clinical care generally must be licensed in the state in which the study subject is located, but it is less clear whether the principal investigator or sub-investigator must be so licensed.

An investigator of a U.S. Food & Drug Administration (FDA) regulated clinical trial, means, in the context of a drug of biological clinical trial, an individual who actually conducts a clinical investigation (*i.e.*, under whose immediate direction the drug is administered or dispensed to a subject). In the event an investigation is conducted by a team of individuals, the investigator is the responsible leader of the team. "Subinvestigator" includes any other individual member of that team.[9] In the context of a medical device clinical trial, an investigator an individual who actually conducts a clinical investigation, that is, under whose immediate direction the test article is administered or dispensed to, or used involving, a subject, or, in the event of an investigation conducted by a team of individuals, is the responsible leader of that team.[10] In either case, the investigator has primary responsibility for the administration of the investigational product and ultimately conduct of the clinical trial.

FDA explains in the applicable guidance that when conducting clinical trials for which drugs, including biological products, under 21 CFR § 312 and of medical devices under 21 CFR § 812, are being investigated, an investigator is responsible for:

- Ensuring that a clinical investigation is conducted according to the signed investigator statement for clinical

investigations of drugs, including biological products, or agreement for clinical investigations of medical devices, the investigational plan, and applicable regulations;
- *Protecting the rights, safety, and welfare of subjects under the investigator's care*; and
- Controlling drugs, biological products, and devices under investigation.[11]

As part of protecting the rights, safety, and welfare of a study subject under the investigator's care, investigators are expected to:
- Provide reasonable medical care for study subjects for medical problems arising during participation in the trial that are, or could be, related to the study intervention;
- Provide reasonable access to needed medical care, either by the investigator or by another identified, qualified individual (*e.g.*, when the investigator is unavailable, when specialized care is needed); and
- Adhere to the protocol so that study subjects are not exposed to unreasonable risks.[12]

The responsibilities of an investigator clearly contemplate providing clinical care outside the context of a specific protocol, which necessarily includes exercising clinical decision-making—a hallmark of medical practice. FDA has noted, "During a subject's participation in a trial, the investigator (or designated subinvestigator) should ensure that reasonable medical care is provided to a subject for any adverse events, including clinically significant laboratory values, related to the trial participation."[13] Providing clinical care to a study subject by an investigator, therefore, logically requires that the investigator be licensed in the state in which the study subject is located (even if the clinical services are being provided *via* telehealth).

## Delegation of Clinical Duties

Investigators routinely delegate specific duties required under an applicable protocol. Nonetheless, when tasks are delegated by an investigator, the investigator is responsible for providing adequate supervision of those to whom tasks are delegated.[14] While FDA assesses the adequacy of supervision by an investigator by probing: (1) whether individuals who were delegated tasks were qualified to perform such tasks, (2) whether study staff received adequate training on how to conduct the delegated tasks and were provided with an adequate understanding of the study, (3) whether there was adequate supervision and involvement in the ongoing conduct of the study, and (4) whether there was adequate supervision or oversight of any third parties involved in the conduct of a study to the extent such supervision or oversight was reasonably possible,[15] state licensure boards on the other hand, concern themselves with whether the clinical procedures performed are within the clinicians scope of practice and, if applicable, the existence and sufficiency of a collaborative practice agreement.

If, for example, a physician assistant (PA) is providing in-home clinical trial related services to a study subject located in Alabama, the PA and the physician would be required to possess licenses to provide clinical care by their respective Alabama licensure boards. Moreover, Alabama provides, "There shall be no independent unsupervised practice by an assistant to physician who is granted a license to practice as an assistant to physician."[16] The qualifications for a supervising physician are set forth in the Board's rules and require, among other things, that the physician be licensed in the State of Alabama and be regularly engaged in the full-time practice of medicine.[17] If the "physician [is] not regularly engaged in the full-time practice of medicine and/or in the circumstance where the physician and the physician assistant seeking registration are each employees of a legal entity other than a professional partnership, medical professional corporation, medical

professional association or physician practice foundation" the PA must demonstrate to the Board that the requisite supervisory relationship exists between the proposed supervising physician and the PA based on a series of factors set forth in the Board's rules.[18] Under Alabama law, "physician supervision" is defined, in relevant part, to mean "[a] formal relationship between a licensed assistant to a physician and a licensed physician under which the assistant to the physician is authorized to practice as evidenced by a written job description approved in accordance with this article."[19] Under the Board's rules, the job description must be signed by both the PA and the supervising physician, submitted with the PA's completed application for registration.[20]

Not only must supervisory requirements be met, if applicable, in the state in which a study subject is located, but a number of states explicitly address whether such supervision may be provided remotely. In Alabama, for example, the supervising physician is not required to provide direct on-site supervision of the PA; however, the supervising physician must provide the professional oversight and direction required by the Board's rules and guidelines, and the requirements must be outlined in the registration agreement if the PA is practicing off-site.[21]

## Telehealth Practice Standards

In addition to licensure and supervisory requirements, clinicians providing clinical services in the context of a clinical trial must abide by the applicable state's telehealth practice standards. Clinicians must comply with the modality requirements of the state in which the study subject is located, for example. In Maine, "telemedicine," is defined by the medical board, means the practice of medicine or the rendering of health care services using electronic audio–visual communications and information technologies or other means, including interactive audio with asynchronous store-and-forward transmission, between a licensee in one location and a patient in another location with or without an intervening health care provider. Telemedicine includes asynchronous store-and-forward technologies, remote monitoring, and real-time interactive services, including teleradiology and telepathology. Telemedicine shall not include the provision of medical services only through an audio-only telephone, e-mail, instant messaging, facsimile transmission, or U.S. mail or other parcel service, or any combination thereof.[22] Similarly, the Kansas Telemedicine Act, defines "telemedicine," including "telehealth," to mean the delivery of healthcare services or consultations while the patient is at an originating site and the healthcare provider is at a distant site. Telemedicine shall be provided by means of real-time two-way interactive audio, visual, or audio–visual communications, including the application of secure video conferencing or store-and-forward technology to provide or support healthcare delivery, that facilitate the assessment, diagnosis, consultation, treatment, education, and care management of a patient's healthcare. "Telemedicine" does not include communication between:

(A) Healthcare providers that consist solely of a telephone voice-only conversation, email or facsimile transmission; or

(B) a physician and a patient that consists solely of an email or facsimile transmission.[23]

In addition to modality considerations, clinicians must abide by any state-specific disclosure and identity confirmation requirements. For example, The Kansas State Board of Healing Arts addresses patient identify verification by requiring that a licensee using telemedicine in the provision of healthcare services to a patient (whether existing or new) take appropriate steps to establish and maintain the licensee–patient relationship. The Board stresses the importance of each licensee using telemedicine to verify the

identity and location of the patient, and, provide the licensee's name, location, and professional credentials to the patient. Licensees prescribing medication, including controlled substances, by means of telemedicine are expected to comply with all state and federal laws, including licensure. When prescriptions *via* telemedicine are permissible, the licensee should implement measures to uphold patient safety in the absence of traditional physical examination. Such measures should guarantee that the identity of the patient and provider are clearly established and there is detailed documentation for the clinical evaluation and resulting prescription. Measures to assure informed, accurate, and error prevention prescribing practices are encouraged.[24]

In Maryland, for example, applicable regulations require that a telehealth practitioner shall develop and follow a procedure to verify the identification of the patient receiving telehealth services.[25]

The majority of states do not state *how* to accomplish patient identification, but require reasonable mechanisms.

## Telehealth Informed Consent

In addition to the standard informed consent requirements applicable to clinical trials,[26] a number of states have specific telehealth informed consent requirements. For example, Cal. Bus. & Prof. Code § 2290.5 provides:

> (b) Prior to the delivery of health care via telehealth, the health care provider initiating the use of telehealth shall inform the patient about the use of telehealth and obtain verbal or written consent from the patient for the use of telehealth as an acceptable mode of delivering health care services and public health. The consent shall be documented.
>
> (c) Nothing in this section shall preclude a patient from receiving in-person health care delivery services during a specified course of health care and treatment after agreeing to receive services via telehealth.

Entities utilizing telehealth are well advised to review and institute applicable telehealth consent requirements in addition to the standard informed consent required for clinical trials.

## Conclusion

Although several companies have emerged that provide clinical trial services and leverage telehealth in addition to providing in-home clinical services, a host of compliance considerations must be addressed for such entities to enter the market without undertaking substantial risk. Corporate structure and telehealth practice standards must be reviewed, understood, and implemented if the hybrid clinical trial model will sustain a compliance audit and survive in the long run.

### Endnotes

1. *See* Tex. Occ. Code § 165.156 (making it unlawful for any individual, partnership, trust, association or corporation by use of any letters, words, or terms, as an affix on stationery or advertisements or in any other manner, to indicate the individual, partnership, trust, association or corporation is entitled to practice medicine if the individual or entity is not licensed to do so).
2. While Texas's corporate practice of medicine rule (Tex. Admin. Code § 177.17) provides for explicit exceptions to the prohibition under subsection (b), these explicit exceptions are limited to hospitals, the federal government, the military, private non-profit medical schools, school districts, state institutions, and rural health clinics, as well as specified Hospital Districts within the State of Texas.
3. *See Midtown Medical Group, Inc., v. State Farm Mutual Auto Insurance Co.*, 220 Ariz. 341 (Ariz. Ct. App. 2008).
4. *See* Ariz. Rev. Stat. Ann. § 32-1401.
5. Colo. Rev. Stat. Ann. § 12-36-117(m).
6. Utah Code Ann. § 16-11-8(1)(a); see also Utah Code Ann. § 16-11-7.
7. Utah Code Ann. § 16-11-2(3)(a).
8. *See* Colo. Rev. Stat. Ann. § 12-36-134.
9. *See* 21 CFR § 312.3(b).
10. *See* 21 CFR § 812.3(i).
11. *See* 21 CFR § 312.60; 21 CFR § 812.100; FDA, Guidance for Industry Investigator Responsibilities—Protecting the Rights, Safety, and Welfare of Study Subjects (Oct. 2009), *https://www.fda.gov/media/77765/download*.
12. FDA, Guidance for Industry Investigator Responsibilities—Protecting the Rights, Safety, and

Welfare of Study Subjects (Oct. 2009), *https://www.fda.gov/media/77765/download*.

13. *Id*.
14. *Id*.
15. *Id*.
16. Ala. Code § 34-24-295.
17. Ala. Admin. Code R. 540-X-7-.17 (Qualifications of The Supervising Physician--Physician Assistants (P.A.)).
18. See Ala. Admin. Code R. 540-X-7-.22 (Physician Assistants (P.A.) Not Employed By Supervising Physician/Physician Not In Full-Time Practice).
19. Ala. Code § 34-24-290(6); *see* Ala. Admin. Code R. 540-X-7-.01(10) (regulation containing similar definition of "physician supervision" to the statute).
20. Ala. Admin. Code R. 540-X-7-.15(3).
21. Ala. Code § 34-24-290(6); Ala. Admin. Code R. 540-X-7-.01(10).
22. Maine Department of Professional and Financial Regulation, Board of Licensure in Medicine, Telemedicine Standards of Practice, *https://www.maine.gov/md/sites/maine.gov.md/files/inline-files/Chapter_6_Telemedicine%20.pdf*.
23. *See* K.S.A. § 40-2,211(a)(5).
24. K.S. Bd. Healing Arts, Telemedicine.
25. Md. Code Regs. 10.32.05.04.
26. *See* 21 CFR part 50.

# What's in Your Pocketbook? The Value and Necessity of Compliance Program Effectiveness Reviews

**Roz Cordini**

**Roz Cordini, JD, MSN, RN, CHC, CHPC**, is a senior vice president and director of coding & compliance services with Coker Group. Ms. Cordini leads the coding & compliance service line to focus on OIG program compliance, including compliance program development, compliance effectiveness reviews, compliance investigations, physician compensation governance procedures, and governance education.

Compliance program effectiveness continues to be a buzz phrase in compliance programs and in the compliance industry in general. Undeniably, governmental enforcement activity highlights its continued importance. The notion of an effective compliance program has been in effect since the *Federal Sentencing Guidelines*, chapter 8,[1] was published in 1991. That document provides the fundamental framework for advising healthcare organizations on ensuring an effective compliance program is in place and further provides for "…periodically evaluat[ing] the compliance program's effectiveness."[2]

On June 1, 2020, the United States Department of Justice (DOJ) Criminal Division issued an updated guidance document, *Evaluation of Corporate Compliance Programs.*[3] Despite such robust guidance, there continues to be significant compliance concerns across the healthcare industry, as evidenced by ongoing DOJ settlements, new corporate integrity agreements (CIA), and other findings and activities.

## Enforcement Activity

On February 1, 2022, the Justice Department released its annual report on False Claims Act settlements and judgements for its fiscal year 2021.[4] The DOJ claims that the $5.6 Billion in recoveries for 2021 are the largest since 2014 (and the second largest amount recorded overall). And of the total, $5 Billion related to healthcare recoveries. On review, it's clear that all sectors are affected—hospitals, physicians, laboratories, medical device and pharmaceutical companies, managed care providers, hospice organizations and pharmacies.

The cases highlighted in the report are of particular interest in terms of the high dollars recovered related to individual settlements. Opioid manufacturers were involved in a $600 Million global resolution of civil and

criminal liability related largely to the promotion of opioid addiction treatment and opioids themselves. Nearly $500 Million of the total was recovered from two companies, Indivior and Purdue.

2021 also saw the continued enforcement related to improper ICD10 diagnosis coding resulting in inflated risk scores for Medicare Advantage beneficiaries. Specifically, Sutter Health paid $90 Million to resolve allegations that it knowingly submitted improper and unsupported diagnosis codes to inflate risk scores of patients participating in Medicare Advantage plans and Sutter Health. Similarly, $6.3 Million was paid by Kaiser Foundation Health Plan of Washington for alleged similar activity. Medicare Advantage diagnosis coding enforcement activity is not new.[5,6,7] Any healthcare organization that participates in Medicare Advantage plans should have this issue on their radar, in their compliance risk assessments and potentially in their annual Compliance Workplans.

Unlawful Kickbacks were also highlighted, including a $160 Million settlement with a mail-order diabetic testing supply company that allegedly provided no cost or "free" diabetic testing glucometers to Medicare beneficiaries as well as routinely waiving or not making reasonable efforts to collect beneficiary co-payments.

A quick Web search can quickly identify various DOJ settlements and CIAs illustrating the types of compliance concerns being addressed through these investigations and settlements. Recently, the DOJ announced a $22 million settlement with the University of Miami to resolve, among other things, allegations related to improper billing for off-campus provider-based facilities.[8] Here, the DOJ alleged that the University knowingly engaged in improper billing by failing to give Medicare beneficiaries who visited those provider-based facilities the required beneficiary notice of co-insurance liability.[9,10]

A brief review of enforcement activity since late 2018 reveals resolutions of alleged noncompliant activity, including inappropriate inpatient admissions ($260M settlement)[11]; inappropriate billing of modifier 59 in orthopedic surgery ($12.5M settlement)[12]; greater than fair market value compensation from a health system to a cardiovascular surgery group ($46M)[13]; and inappropriately billing an E/M on the same day as a procedure ($1.85M),[14] to name just a few. In almost all areas health care organizations operate in, we see the potential for risk.

How can this type of enforcement activity be used by organizations in evaluating risk? When was the last time the organization audited its collections process to ensure reasonable attempts have been made to collect co-pays? What types of new equipment is available to physician practices and how have patients been encouraged to have that equipment used? Have tests been provided at no-cost? How accurate is diagnosis coding in the organization? Has there been any audit activity around Hierarchical Condition Coding, particularly for organizations participating in risk-based contracts? The applicability of enforcement activity is not necessarily direct. It is critically important for organizations to use knowledge of enforcement activity specifically related to the actual enforcement activity, but also in critically thinking about how a similar issue could arise given existing business operations.

Notably, whistleblowers brought forward many of these allegations within the referenced organizations. In its 2021 report, the DOJ provides that $1.6 Billion of the total $5.6 Billion recovered arose from qui tam lawsuits. Arguably, evaluating each compliance program's effectiveness may have identified potential concerns before governmental investigators became involved.

## What Constitutes a Well-Designed Compliance Program?

According to the DOJ, a well-designed compliance program is comprehensive, sends a clear message of zero tolerance

for misconduct regardless of one's position within the company, and is well-integrated into day-to-day operations. The performance of a compliance risk assessment is the foundation of the program, identifying specific risk areas for use in tailoring the annual compliance work plan.

### Policies and Procedures

Key to operationalizing a compliance program is developing and implementing compliance policies and procedures, including a Code of Conduct that sets out the organization's commitment to compliance and expectation of adherence to the compliance program and compliance with the law. Further, policies and procedures should reinforce the culture of compliance within the organization and be easily accessible to all employees.

### Training and Communications

Training also plays a critical role in designing a compliance program. In addition to general training, employees should receive training based upon risks and actual compliance issues identified throughout the prior year and associated lessons learned. Employees should be tested on their comprehension and certify they understand the compliance policies and procedures and acknowledge their duty to report known or suspected compliance concerns as a condition of employment. Additionally, senior leadership should message employees about their zero-tolerance position on misconduct.

### Hotline and Investigation Process

The key to ensuring this element is met is ensuring that a confidential reporting system that is well-publicized to all employees exists and that they feel they have a mechanism to report concerns or seek guidance without the fear of retaliation. The DOJ guidance provides that having such an established reporting mechanism in place is "highly probative" of whether the organization can prevent and detect misconduct in an effective manner.[15] Consider the whistleblower activity described above and whether such a mechanism for reporting was available and, if reported, timely addressed. Further, appropriate personnel should conduct investigations in an objective, independent, timely manner and should assign accountability for follow-through with recommendations.[16]

### Vendor Management

Using third parties is prevalent and necessary for the functioning of many organizations. A well-designed compliance program will ensure the performance of due diligence around the selection of vendors, including reputational and relationship diligence. Documenting the business rationale for the relationship should exist with clear articulation in the agreement of the services to be provided and documentation of the fair market value of the proposed compensation.

### Mergers and Acquisitions

With mergers and acquisitions in healthcare continuing to be an important business strategy, how and to what extent an organization subjects a target to compliance diligence reflects how well-designed its compliance program is. Failure to identify wrongdoing in diligence may permit misconduct to continue at the acquiring organization undetected and may subject the acquiring organization to civil and criminal liability, business losses, and reputational harm.

Finally, post-acquisition activity is equally important. Employing a solid post-acquisition integration plan ensures the acquiring organization successfully addresses compliance concerns identified in the diligence process and provides a roadmap for continued success.

## Is the Program Being Applied Earnestly and in Good Faith?

Even the most robust structured compliance program may fail when implementation is

ineffective, absent, or lax. One barrier to effective implementation surrounds the compliance officer's stature and authority within the organization. Without the proper authority and a seat at the table, resources may be limited, and ineffective or corrective action inconsistently applied. Where the compliance officer is uninvolved in key strategic discussions, a tone-at-the-top issue may exist. Of utmost importance, regardless of the level of the compliance officer, the compliance officer must have direct access to the Board and be allowed to function independently. "…[I]f a compliance program is to be truly effective, compliance personnel must be empowered within the company."[17]

## Commitment by Senior and Middle Management

The DOJ reiterates that an effective compliance program requires a high-level commitment by senior leadership. An example of this may include leaders messaging employees about the importance of compliance and that misconduct will not be tolerated, regardless of one's position. Disparate treatment in action sets a low tone about compliance within the organization and sends a message that compliance is important for some but not all. Ultimately, the Board and senior leadership are responsible for setting the tone at the top. Further, the governing body is responsible for ensuring senior executives set the correct tone, including holding them accountable for doing so.[18] When evaluating an organization's commitment to compliance, the DOJ guidance instructs its prosecutors to look for "rigorous adherence by example" of senior leaders when investigating misconduct and concrete examples of modeling proper behavior to subordinates.[19]

## Individual Accountability

Another important consideration for organizations pertains to individuals being held accountable for their involvement in compliance issues, particularly senior executives. The Yates Memo was delivered by former Deputy Attorney General Sally Yates in September 2015, establishing an exacting cooperation credit policy requiring corporations to provide all relevant facts about the individuals involved in corporate misconduct to the DOJ in order to be eligible for any cooperation credit, in both criminal and civil cases, as well as a distinct focus on holding individuals accountable for their involvement and failure of oversight.[20]

> [A]bsent extraordinary circumstances or approved departmental policy, the Department will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation.[21]

In November 2018, Deputy Attorney General Rod J. Rosenstein outlined a revised policy in his remarks at the International Conference on the Foreign Corrupt Practices Act Annual Meeting.[22] In his remarks, he reiterated the importance of holding corporations responsible for wrongdoing, but announced a relaxed posture with respect to civil cases, meaning, prosecutors will have more discretion and are not required to use the previous all or nothing approach. Despite the revisions, holding individuals accountable remains in effect.

The Justice Department's most recent report on the 2021 False Claims Act settlements confirms this. In the Purdue settlement previously discussed, separate from the general unsecured bankruptcy claim in the amount of $2.8 Billion to resolve allegations that it promoted opioids to providers it knew were prescribing for medically unnecessary and unsafe use, *individual* Sackler family members who served as board members and were shareholders agreed to resolve civil False Claims Act allegations in the amount of $225 Million

for allegedly approving a new intensified marketing program aimed causing unsafe, medically unnecessary and ineffective to "extreme" high volume prescribers. Senior executives and board members must appreciate the importee of their role in compliance program oversight.

### Incentives and Disciplinary Measures

Incentives and discipline motivate employees to promote compliance and avoid misconduct; however, they must be meaningful and consistently applied. Incentives often range from a merit increase based upon compliance as an element of a performance evaluation or a factor considered when giving promotions or issuing bonuses. Doing so reinforces the importance of compliance within the organization and incents such behavior from all levels. Additionally, well-publicized disciplinary measures that are consistently enforced are equally important.

## Does the Corporation's Compliance Program Work in Practice?

The DOJ understands that all misconduct cannot be prevented even with the best compliance program in place. Key to its evaluation, if the organization did not detect the misconduct immediately, is whether it had appropriately focused its activities on high-risk behaviors and whether the compliance program was revised or modified in response to the misconduct. If the compliance program did detect the misconduct, halt the noncompliance, and effectively remediate and self-report the issue, then prosecutors would likely view the organization as having an effective compliance program in place.

## Continuous Improvement

The hallmark of an effective compliance program is its capacity to evolve and improve over time in response to incidents experienced and lessons learned. The DOJ guidance discusses the importance of performing a root-cause analysis when noncompliance occurs. Through this process, an organization can identify where controls failed or were missing, what compliance culture issues may be present impacting compliance effectiveness, and an opportunity to put in place improved controls to prevent a similar problem in the future. This process permits employees and departments involved in the misconduct to the concerns and the importance of their role in preventing noncompliance.

## Conclusion

In summary, an effective compliance program operates in a cycle of continuous improvement. Today's compliance environment requires much more than merely a written compliance program. It involves surveying staff and providers, testing the effectiveness of internal program operations, probing into the follow-through of corrective action plans, and evaluating the program's continued growth based upon newly identified risks and lessons learned. There is no reasonable expectation of perfection. Issues will arise even in deemed low-risk. A proactive approach to evaluating the effectiveness of an organization's compliance program may just be the difference between a thoughtful investment in the organization's compliance health or emptying the entire pocketbook.

### Endnotes

1. United States Sentencing Commission. 2018 Chapter 8, Sentencing of Organizations. *https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8*. Accessed Jul. 13, 2021.
2. *See* fn 1, Sec. 2.1(5)(B).
3. U.S. Department of Justice Criminal Division Evaluation of Corporate Compliance Programs, 2020. Guidance Document. *https://www.justice.gov/criminal-fraud/page/file/937501/download*. Accessed Jul. 13, 2021.
4. *https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year*. Accessed Feb. 10, 2022.
5. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/medicare-advantage-provider-pay-30-million-settle-alleged-overpayment-medicare-advantage*. Accessed Jul 13, 2021.

6. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/medicare-advantage-provider-pay-63-million-settle-false-claims-act-allegations*. Accessed Jul 13, 2021.
7. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/usao-cdca/pr/medicare-advantage-provider-pay-270-million-settle-false-claims-act-liabilities*. Accessed February 10, 2022.
8. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/university-miami-pay-22-million-settle-claims-involving-medically-unnecessary-laboratory*. Accessed May 10, 2021.
9. 42 CFR 413.65(g)(7).
10. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/university-miami-pay-22-million-settle-claims-involving-medically-unnecessary-laboratory*. Accessed Jul 13, 2021.
11. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/hospital-chain-will-pay-over-260-million-resolve-false-billing-and-kickback-allegations-one*. Accessed Jul 13, 2021.
12. U.S. Attorney's Office Eastern District of Pennsylvania. Press release. *https://www.justice.gov/usao-edpa/pr/coordinated-health-and-ceo-pay-125-million-resolve-false-claims-act-liability*. Accessed Jul 13, 2021. Note: The hospital had several external audits identifying the issue and recommending the practice cease and that claims be repaid. These recommendations were allegedly not implemented.
13. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/california-health-system-and-surgical-group-agree-settle-claims-arising-improper-compensation*. Accessed Jul 13, 2021.
14. U.S. Department of Justice Office of Public Affairs. Justice news. *https://www.justice.gov/opa/pr/skyline-urology-pay-185-million-settle-false-claims-act-allegations-medicare-overbilling*. Accessed July 13, 2021.
15. *See* n.5.
16. The DOJ guidance recommends setting timing standards and metrics and measuring and reporting on these metrics.
17. Ibid. p. 10.
18. To that end, governing bodies should reflect on how they are ensuring the correct tone is being set within the organization. As a best practice, Boards should periodically meet in closed session with their compliance officer and talk about how the program is running.
19. *See* n.1, p. 9.
20. Memorandum from Sally Quillian Yates, Deputy Att'y Gen., US Dep't of Justice to All US Att'ys et al., Individual-Accountability for Corporate Wrongdoing (Sept. 9, 2015). *https://www.justice.gov/archives/dag/file/769036/download*. Accessed February 10, 2022.
21. Ibid, p. 2.
22. Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act. Justice news (Nov. 29, 2018). *https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0*. Accessed February 10, 2022.

# High Impact, Unique Risks—What Compliance Professionals Need to Know About the 340B Drug Discount Program

**James Junger**

In late 2021, I was fortunate to be asked to speak to a group of law students who were considering careers in health law. When one student asked me what it was like starting out in a field where I had no prior experience, I jumped at the opportunity to use one of my favorite metaphors: "Learning a new field is like looking up at a starry sky. At first, all you can see are the brightest stars. After a while, your eyes start to adjust, and stars that were invisible a few minutes ago come into view. As you take on new projects and learn new things, you form connections, turning that starry sky into constellations that you can use to better understand exactly where you're standing."

In the starry sky that is health law, somewhere between the Big Dipper and Pyxis[1] lies the 340B Drug Discount Program (340B Program). Under the 340B Program, safety-net hospitals and grant-supported clinics are entitled to significant discounts on outpatient drugs. When these costs are reduced, participating providers (called Covered Entities) are able to "stretch scarce Federal resources as far as possible, reaching more eligible patients and providing more comprehensive services."[2] Although it is an overgeneralization, the 340B Program essentially requires participating drug manufacturers[3] to offer their "best price" to Covered Entities and limits the rate at which manufacturers can raise those prices. In short, instead of paying over their federal grant funds or enhanced Medicare/Medicaid payments to drug companies, Covered Entities can use that money to support their safety-net missions. Often the impact is significant, contributing substantially to a Covered Entity's bottom line.

Like many areas of health care, the 340B Program has its own vocabulary. A "Covered Entity" that enrolls in the 340B Program is entitled to purchase "Covered Outpatient Drugs" at (or below) the 340B "Ceiling

**James Junger, Esq., CHC** is a healthcare compliance and pharmacy attorney with Hall Render, the nation's largest law firm focused exclusively on the needs of health care clients. James can be reached at jjunger@hallrender.com.

Price." The Covered Entity can administer or dispense 340B-priced drugs to its "Eligible Patients" and retain any margin between its purchase price and sale price. It can hold its Covered Outpatient Drugs in a "Physical Inventory," or, using a process known as "Retroactive Replenishment" facilitated by a "Third-Party Administrator," to maintain a "Virtual Inventory." An order or a prescription for a Covered Outpatient Drug may be written by an "Eligible Prescriber" in the Covered Entity's "Parent Site" or a "Child Site." The Eligible Patient may receive their Covered Outpatient Drugs from the Covered Entity itself or from a "Contract Pharmacy."

This article is intended to be a compliance professional's star chart for this 340B constellation. It identifies the basics of the program, the authorities underlying it, and the risks that come along with 340B Program noncompliance. It also describes some common implementations and current challenges faced by Covered Entities, then suggests compliance touchpoints using the familiar Seven Elements framework.

## The Basics of the 340B Program

### Authorities Governing the 340B Program

The 340B Program is created by statute (42 U.S.C. § 256b) and administered by the Health Resources and Services Administration (HRSA), principally through its Office of Pharmacy Affairs (OPA). Although HRSA is responsible for administering the 340B Program, its authority to issue legally binding regulations is quite limited; the regulations at 42 C.F.R. Part 10 address only a few discrete aspects of the 340B Program. Despite these limitations, over the past three decades, HRSA has published a wide array of subregulatory guidance interpreting the 340B statute and regulations regarding Covered Entities and manufacturers. This guidance is found in the Federal Register and in letters and other materials posted on HRSA's Web site. Information on specific Covered Entities can be found on the 340B Office of Pharmacy Affairs Information System (called "OPAIS"), at *https://340Bopais.hrsa.gov*. Covered Entities are required to register through OPAIS, and maintain accurate registrations for their Parent Sites, Child Sites, and Contract Pharmacies. Registration periods occur during the first 15 days of each calendar quarter.

In addition, HRSA has contracted with a 340B "Prime Vendor," currently Apexus, whose responsibilities include providing education and guidance for Covered Entities and manufacturers. The Prime Vendor's Web site, *https://www.340Bpvp.com*, contains a host of good-quality resources, including Frequently Asked Questions which, while not authoritative, are reviewed by HRSA before posting.

### What Covered Entities May Not Do: Diversion and Duplicate Discounts

While there is some nuance in the ways that each different Covered Entity type may implement the 340B Program (described in further detail below), all Covered Entities are subject to two broad prohibitions:

- Diversion: Covered Entities may not use 340B drugs for anyone except their own Eligible Patients.[4]
- Duplicate Discounts: Covered Entities may not request Medicaid reimbursement for a 340B-priced drug if the state Medicaid program will receive a rebate for the same drug under the Medicaid Drug Rebate Program.[5]

Covered Entities are subject to audit by HRSA and manufacturers to verify their compliance with these and other program responsibilities. Unlike many areas of health care, a Covered Entity is typically not subject to civil monetary penalties or fines for noncompliance, but it will be expected to implement an effective corrective action plan, repay any manufacturers affected by the noncompliance, and

may be ordered to pay interest. Covered Entities may also be removed from the program for "systematic and egregious" violations.[6]

## Covered Entities and Eligible Patients

340B Program participation is limited to government-owned or non-profit hospitals and clinics that meet certain eligibility criteria.[7] Eligible hospitals include critical access hospitals as well as disproportionate share (DSH) hospitals, children's hospitals, freestanding cancer hospitals, sole community hospitals, and rural referral centers. With the exception of critical access hospitals, a hospital's eligibility is based on, among other things, its disproportionate share percentage exceeding statutory thresholds.[8] Hospitals must continuously meet the DSH requirement, as reflected on their most recent as-filed Medicare cost report.

Eligible clinics include federally qualified health centers (FQHC) and FQHC look-alikes, as well as entities that receive grants under certain federal programs, such as family planning clinics, Ryan White clinics, hemophilia treatment centers, and black lung clinics.

As noted above, Covered Entities are only permitted to administer or dispense 340B-priced drugs to their "Eligible Patients." There is no statutory or regulatory definition of an "Eligible Patient," and Covered Entities commonly adopt policies to define the criteria they will apply when determining whether a person is an Eligible Patient. Under 1996 HRSA guidance,[9] a Covered Entity must at least:

- Establish a relationship with the patient such that it maintains a record of their care;
- Provide health care services, other than the dispensing of a drug, to the patient: (a) through a health care professional who is employed by or under contract with the Covered Entity; (b) consistent with the scope of its grant (if the Covered Entity is a grantee).

In addition, under 1994 HRSA guidance, the person must have received the qualifying care at the Covered Entity's Parent Site (*i.e.*, a reimbursable location within the four walls of the Covered Entity facility) or at a registered Child Site. A Covered Entity may register an outpatient facility as a Child Site if the facility incurs reimbursable costs on the Covered Entity's most recent as-filed cost report.[10]

## Covered Outpatient Drugs and Orphan Drugs

Mandatory 340B pricing applies only to Covered Outpatient Drugs, and although it is fundamental to the 340B Program, this term is not defined directly in the 340B statute. Instead, it relies on the definition from the related Medicaid Drug Rebate Program.[11] At a high level, the term includes separately payable[12] prescription drugs and biologicals other than vaccines. Drugs that are administered to patients in the Covered Entity facility are included in this definition, and it is common for Covered Entities to ensure that their 340B Program implementation covers clinics that routinely administer infused drugs, such as cancer centers.

Compliance professionals who work for sole community hospitals, rural referral centers, and freestanding cancer hospitals should be aware that drugs with an "orphan drug" designation are not considered Covered Outpatient Drugs when used by these Covered Entity types.[13]

## Common 340B Program Implementations

In its most basic form, a transaction involving a 340B-priced drug is fairly simple: A patient visits their physician, who prescribes a Covered Outpatient Drug. The patient takes that prescription to the Covered Entity's pharmacy, and the pharmacy fills the prescription with a product that it had previously purchased from a participating manufacturer at the 340B price. The patient (or their insurer) pays

the pharmacy for the drug. The Covered Entity retains any margin between the price it charges the patient or their insurer and the price it paid the manufacturer.

Many variations on this structure exist. For instance, 340B pricing may be available when the drug is administered in the Covered Entity's facility, or when the pharmacy dispenses drugs from its general stock, or when the pharmacy is not owned or controlled by the Covered Entity. As long as the appropriate compliance structures are in place, the Covered Entity has significant freedom in designing its own 340B Program implementation.

### Virtual Inventories

In most cases, it will be impractical for a Covered Entity to maintain separate physical inventories of 340B and non-340B drugs. Instead, using specialized software, Covered Entities will compare registration, prescribing, drug purchasing, and dispensing data to determine which administrations/dispenses were to Eligible Patients. Then, it orders an equal number of drugs at the 340B price. This is known as a "retrospective replenishment" model, and the Covered Entity is said to maintain a "virtual inventory." Although it would be possible for a Covered Entity to build systems to do this analysis, most choose to contract with vendors who have expertise in the area, known as "third-party administrators."

With regard to virtual inventories, compliance risks may arise if a Covered Entity does not have a robust system in place to ensure that the correct data is being fed into its third-party administrator software.

### Contract Pharmacies

Covered Entities are not required to operate a retail pharmacy to take full advantage of the 340B Program. Instead, since the very beginning of the program, they have entered into contracts with existing pharmacies to dispense 340B-priced drugs to their Eligible Patients. In most cases, a "Contract Pharmacy" will operate on a virtual inventory basis, and the Covered Entity will purchase replenishment inventory on a "ship-to/bill-to" basis.

Beyond providing retail pharmacy services, the Contract Pharmacy structure enables many Covered Entities to access 340B pricing for specialty drugs. These are drugs that are distributed only through specially equipped pharmacies (called specialty pharmacies) because, for example, the drugs require special storage and handling or because they treat especially severe conditions. Few Covered Entities have the resources to support, or patient volumes to justify, creating their own specialty pharmacies.

Although it is beyond the scope of this article, compliance professionals should be aware that since the summer of 2020, some participating drug manufacturers have challenged the contract pharmacy structure, and some are no longer facilitating ship-to/bill-to orders. These manufacturer actions have been the subject of HHS enforcement efforts and manufacturer lawsuits.

## Compliance Touch Points

Many organizations adopt a compliance program to help it avoid civil or criminal penalties for unlawful conduct. In the case of 340B Program violations, the risk of such penalties is quite low for Covered Entities,[14] and perhaps as a result, Compliance often does not have clear line-of-sight on 340B operations. However, the 340B Program intersects with potentially high-risk areas such as: Medicare cost report rules; billing and coding rules for Medicare, Medicaid, Medicaid Managed Care Organizations and other private insurers; state and federal controlled substances laws; and state licensing laws. As a result, many Covered Entities would benefit from more active Compliance involvement in their 340B Program implementations. Below are examples of how the familiar Seven Elements framework can be applied to the 340B Program.

## Policies and Procedures

Due in part to HRSA's limited regulatory authority, Covered Entities have significant freedom to design a 340B Program implementation that is appropriate for their situation. HRSA encourages Covered Entities to implement policies and procedures to guide their 340B operations, and HRSA will request copies of these documents during an audit.[15]

In many cases, a Covered Entity's 340B operations are led by pharmacy personnel. Although many pharmacists prepare handbooks, protocols, and the like to guide pharmacy operations within their organizations, they may not have formal training or experience in drafting, updating, and managing compliance policies. Compliance professionals could consider assisting 340B Program personnel with reviewing and updating their policies and procedures to ensure that they accurately reflect the organization's approach to 340B compliance and implementation. Close collaboration between pharmacy/340B personnel and compliance personnel will help ensure that the pharmacists' substantive knowledge combined with the compliance professional's experience will lead to accurate and reliable documentation.

## Compliance Officer and Compliance Committee; Monitoring and Auditing;[16] Open Lines of Communication; Well-Publicized Disciplinary Guidelines

Many Covered Entities would benefit from active, intentional collaboration between Compliance and pharmacy. Implementing an effective compliance program is a group effort, with the compliance activities taking place throughout the organization and the compliance officer acting as their "focal point."[17] Adopting this structure for the 340B Program, where primary responsibility for ensuring compliance with 340B Program requirements through monitoring, auditing, and other activities is vested with those responsible for implementing the Program, can be highly effective.

As noted above, many Covered Entities vest responsibility for the 340B Program with pharmacy personnel who have specialized knowledge, training, and experience in pharmacy and pharmacy management. Often, these individuals develop processes that work for their Covered Entities, solve problems as they arise, and call on contacts across the organization to assist as needed. In many cases, though, 340B Program personnel develop solutions to what are effectively "solved problems." For instance, a pharmacist may feel that they are asking for a favor when, to recertify eligibility for an existing Child Site, they need to request a copy of the hospital's Medicare cost report. Similarly, those responsible for a 340B Program implementation may develop a working document that describes how the Covered Entity identifies its Eligible Patients, but may not have the resources to have the document adopted as a policy.

Compliance personnel can help their Covered Entity implement the 340B Program by bridging gaps between Pharmacy and other areas of the organization and setting the expectation that those responsible for the 340B Program be given access to documents, personnel, and other resources necessary to adequately measure compliance. In addition, compliance personnel can provide education on compliance principles, including the Seven Elements, to act as a force multiplier for their pharmacy personnel's organic compliance efforts. In return, Compliance may expect that Pharmacy participates on the Compliance Committee, reporting on their ongoing compliance efforts to help Compliance get a fuller view of the organization's activities. Compliance can also help by holding individuals across the organization responsible for contributing to 340B compliance activities, with the expectation that a failure to do so is actionable as a violation of policy.

## Training and Education

Since 340B is a highly specialized area, those who work in the field have to develop a good understanding of the laws, regulations, and expectations pertinent to the 340B Program. And, despite this complexity, the 340B Program is characterized by relatively infrequent changes in these rules, at least when compared to the rest of health care.

Compliance can help Pharmacy by becoming educated on the 340B Program so they may actively engage in and oversee 340B compliance activities.[18] In addition, Compliance can help spot any changes in Program expectations by monitoring the HRSA Web site and keeping an eye out for 340B-related topics in industry news.

## Detecting Offenses and Implementing Corrective Action

As noted above, compliance personnel should be informed of routine 340B auditing and monitoring activities. Inevitably, these activities will find instances of noncompliance, and Covered Entities should expect to adopt effective corrective action plans in response. Compliance personnel, with their expertise in assessing systems and guiding corrective action, should contribute to this effort. Compliance personnel should ensure that any corrective action plan is measured for effectiveness, as Covered Entities face additional risk if noncompliance is "knowing[] and intentional[]" or "systemic and egregious[.]"[19]

## Conclusion

The 340B Program may not be the first thought when identifying an organization's compliance risks, but it should not be an afterthought. A well-developed plan for 340B implementation can help safety-net providers keep the doors open and offer better and more comprehensive services to patients. Compliance professionals should consider reaching out to their Pharmacy counterparts and offer their support in ensuring that 340B savings continue to bolster the organization's safety-net mission.

### Endnotes

1. *See* International Astronomical Union, The Constellations (*https://www.iau.org/public/themes/constellations/*) (last accessed February 14, 2022).
2. H.R. Rep. 102-384(II), at 12 (1992).
3. Manufacturers opt in to the 340B Program, as well as the related Medicaid Drug Rebate Program, as a condition of receiving Medicare Part B and Medicaid payments for their products. *See* 42 U.S.C. § 256b(a)(1); 42 U.S.C. § 196r-8(a)(1).
4. 42 U.S.C. § 256b(a)(5)(B).
5. 42 U.S.C. § 256b(a)(5)(A). Note that the responsibility for complying with this prohibition shifts to the states and their Medicaid Managed Care Organizations if the Covered Entity would be paid by the MCO. *See* 42 U.S.C. § 1396r-8(j).
6. 42 U.S.C. § 256b(d)(2)(B)(v)(ii).
7. *See* 42 U.S.C. § 256b(a)(4).
8. Greater than 11.75% for disproportionate share hospitals, children's hospitals, and freestanding cancer hospitals (42 U.S.C. §§ 256b(a)(4)(L)-(M)), and at least 8% for sole community hospitals and rural referral centers (42 U.S.C. § 256b(a)(4)(O)).
9. 61 Fed. Reg. 55,156, 55,157–58 (Oct. 24, 1996).
10. Note that there is a close correlation between this requirement and the Centers for Medicare & Medicaid Services' provider-based requirements at 42 C.F.R. § 413.65.
11. *See* 42 U.S.C. § 256b(b)(1) (cross-referencing 42 U.S.C. § 1396r-8(k)).
12. A drug that is paid and used as part of, or incident to and in the same setting as, a physician, hospital, or other medical service is not a Covered Outpatient Drug.
13. 42 U.S.C. § 256b(e).
14. Manufacturers may be subject to civil monetary penalties of up to $5,000 (adjusted annually for inflation) for overcharging a Covered Entity for a drug subject to the 340B Ceiling Price. 42 U.S.C. § 256b(d)(1)(B)(vi).
15. The 340B Prime Vendor has published a set of template policies for each different Covered Entity type, available at *https://www.340bpvp.com/resource-center/340b-tools*. Compliance professionals should be aware that these and other resources available from the Prime Vendor, while of generally high quality, reflect standards that are in excess of what is legally required for a 340B Program implementation.
16. Many Covered Entities choose to conduct audits, and especially external audits, under the attorney–client privilege.
17. HHS Office of Inspector General, *Compliance Program Guidance for Hospitals*, 63 Fed. Reg. 8987, 8993 (Feb. 23, 1998).

Continued on page 70

ROY SNELL

# An Interview with Joe Murphy, the Godfather of Compliance

**Roy Snell** is the ESG and Sustainability Officer for Osprey ESG Software. Roy is the co-founder of the Heath Care Compliance Association and the Society of Corporate Compliance. He is the author of Integrity Works and The Accidental Compliance Professional.

Attorney Joe Murphy has over 40 years of experience in organizational compliance and ethics. Joe has published over 100 articles and given over 200 presentations in 21 countries. He is Editor of SCCE's Compliance & Ethics Professional magazine and has been recognized with SCCE's Compliance and Ethics award, and received the Concurrences 2021 Antitrust Compliance Awards, Special Award. He was the co-author of the first book on compliance, Sigler & Murphy, *Interactive Corporate Compliance* (Greenwood Press; 1988), and wrote Murphy, Joseph E., Policies in Conflict: Undermining Corporate Self-Policing, 69 Rutgers L. Rev. 421 (2017), *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3685529*.

**Snell:** How did you get into compliance, and when did you recognize that this was a field separate from just being a lawyer?

**Murphy:** My first contact with compliance was in 1976, when I started working in the legal department at a Bell company (one of the AT&T telephone companies). I had been brought in to work on antitrust. The company had major litigation, but also wanted work done on antitrust compliance. So I started with compliance training, using a new, dramatic video called "The Price." Later I picked up some responsibility for the environmental area and started seeing similar compliance patterns to what was happening in antitrust. After that, when the FCPA was enacted, I saw the same patterns in compliance work in response to that new law. I also worked with groups in-house whose job was to deal with competitors. Back then, if you were at a telecom company, the only way to reach customers locally was through the local Bell companies. So we had created groups within the company whose job was to ensure that competitors were treated fairly. It was a mix of all these elements that led me to realize that "compliance" was a discrete subject broader than just the compliance work in one specific field, and doing

compliance work was different from just being a lawyer.

**Snell:** What are the most important personality traits of a compliance professional?

**Murphy:** First, you need a commitment to seeing that the organization does the right thing. You can't be a cheater or cornercutter. An ability to listen—really listen—to people at all levels of the organization is important. Yes, we have to talk with the board and the officers, but if we don't talk with the workers we will not know what is actually going on or what the real culture of a company is. Next, humility is important, so that we can learn and listen. Finally, it is important to have courage - to be able to stand up to a top person with too much power and just say "no."

**Snell:** What are the least desirable personality traits of a compliance professional?

**Murphy:** Two opposite traits—timidity, because it is a tough profession. And arrogance, because you can't succeed if you don't listen to others and think you know everything.

**Snell:** What are the most important elements of a compliance program?

**Murphy:** There are certain elements you must have, or you simply do not have a compliance program. Number one is management commitment. If you don't have that you don't really have a program. Next on my list is having an empowered, independent compliance and ethics officer with line of sight into every part of the company. You need someone to make things happen. The third essential element is addressing incentives. We use incentives because they drive behavior. Poorly designed incentives can cause people to do the wrong thing, and the right incentives can promote a strong, positive culture. Note that none of these includes the items almost everyone discusses - having a code of conduct and doing training. If you have the three I have listed here you will get those others automatically. But if you don't have these three you are setting yourself up for failure.

**Snell:** Some ethicists say, "Go beyond compliance to ethics." What do you think they mean by that? Do you agree?

**Murphy:** I never could understand this. The field is "compliance **and** ethics." This means our message is "do the right thing." Our message is to follow the law and do what is right. People in our field do not need to focus on ethics instead of compliance. There is much more need to study management and psychology. We need to focus on what makes people do what they do and how we can reach them with this message. Also, typically when they say this they are ignoring what the law actually is. They view law as just some empty technical requirements. They do not understand the "why" behind the law, so they do not understand the law. But law is how society decides among competing values. It sets a priority. Merely telling people to be ethical leaves them adrift when, as so often happens, values conflict. So our field has to be about law and compliance. Know and follow what society tells us is required. Understand this first. Then commit to do what is right. You cannot do one without the other.

**Snell:** Do you have to be an attorney to be a compliance professional?

**Murphy:** No. But there are characteristics of being an attorney that are helpful. You need to act professionally, which includes being able to control your emotions and look objectively at the facts. You need to be able to master the facts and learn quickly. A good lawyer knows the importance of listening and not jumping to conclusions. Building on these characteristics, a lawyer can be successful in

compliance and ethics as long as they are curious and open to learning about this as a new field beyond the traditional practice of law. But one does not need to be a lawyer. Compliance and ethics is a multidisciplinary field. You can function well in it if you have a background in HR, internal audit, security, or are good at project management. There are many skills that are valuable in our field. You certainly do not have to be a lawyer.

**Snell:** Should compliance report to the legal department?

**Murphy:** No. Compliance is not the same as the practice of law. Ironically, compliance is closer to HR than to legal in terms of the day-to-day work. If you look at the Sentencing Guidelines' seven steps, they have more in common with HR than with legal. But lawyers and writers sometimes make the enormous mistake of thinking that legal and compliance can only work together if compliance is underneath, controlled by and owned by legal. Yet legal works with all different departments in companies without owning any of them. It has no more need to control compliance than it does to control HR, internal audit, IT, sales, marketing, or anyone else. Lawyers should not be threatened or insecure about compliance and ethics; lawyers should view this function as an important ally.

**Snell:** If you only had had 15 minutes with your organization's board each year as a compliance officer, what would be the most important things to cover?

**Murphy:** I am not sure who would have the guts to say this, but maybe just send them a note saying, "No, I cannot report in 15 minutes a year and do my job. I would only mislead you if I did report and let you think you were discharging your fiduciary responsibility by my doing this." Perhaps, if the board were in the United States, I would report on the *Marchand* decision, explaining how they were setting themselves up to be sued personally for failing to oversee the compliance program and address their key compliance risks. A quarter hour a year is not going to impress any judge in any court. Plus, it will not represent effective oversight of the compliance program.

**Snell:** The US Federal Sentencing Guidelines suggest that an organization with an effective compliance program should be given a break in the penalty phase… should they get into trouble. Is there documented evidence that this has ever occurred? Is there anything the government could do to be more effective at encouraging the implementation of compliance programs?

**Murphy:** The Sentencing Guidelines were a brilliant experiment, and were wildly successful in the US and globally. But they never worked as intended for one major reason: companies in the US do not go to trial in criminal cases. So the idea of the Sentencing Guidelines - giving companies credit for having effective compliance programs - really was picked up by enforcers and embraced in a way that is more effective.

Smart prosecutors and regulators look at a company's compliance program to determine the company's true culpability—does it really deserve to be punished. They then determine how tough to be on the company. They may decide the program was too weak and just prosecute. Or they may say the effort was good, and the company deserves some break, but the program was not what it should have been. Or there may have been a truly rogue employee who covered up the wrongdoing despite the company having a rigorous compliance program, and that company might not be prosecuted at all.

A weakness in the Sentencing Guidelines model was that it was all or

nothing. Either the program got you a specific reduction or it did not. The approach by enforcers is more graduated, recognizing that programs can operate on a spectrum, and some will deserve more recognition than others. So there have been some relatively trivial cases in the courts where programs were considered. But at the enforcement level the cases are few but visible. In FCPA, for example, everyone cites the MorganStanley case. Where the government is falling short and could get better results, is in reporting on actual cases where compliance programs were considered, and telling us, in those cases, what programs failed and the reasons, and what programs merited credit and what was good about them. Of course, they can omit the identities of companies while still sharing the lessons learned. But actual cases would have more impact on companies.

**Snell:** You have been working very hard on promoting antitrust compliance. Why is that? What have you done to try to help? Have your efforts resulted in any changes?

**Murphy:** In antitrust there was animosity by enforcers to compliance programs. First, the enforcement agencies had strong voluntary disclosure programs, so enforcers believed they needed nothing else. Just answer the phone when someone called to report a violation and then prosecute everyone else who was involved in the violation. Also in antitrust there were too many theorists who relied on theory without regard to what actually existed. They still lived in very old-fashioned world where everyone was presumed to be a mindless profit maximizer and all government had to do was determine the so-called optimal penalty and no one would ever break the law again. They played a game of pretend: pretend that corporations were just giant people who made calculated rational decisions. They pretended there were not different types of human beings, or different motivations for violations, or any possibility that people in corporations might actually work to prevent misconduct. Every human was an "econ" motivated only by financial gain. So with this extremely distorted view of companies they were not interested in the idea that there could be groups or constituencies, within organizations that could work to prevent wrongdoing. They could not recognize that there would be people in companies whose purpose was to prevent wrongdoing; after all, the only reason they believed people worked was for the single-minded pursuit of cash.

I did an enormous amount of writing and speaking in this area to challenge this narrow thinking. It was a simple point: governments should help to promote effective compliance and ethics programs. The way to do this was to treat companies that made serious efforts to prevent violations more favorably than those that did not. I started a simple email group dedicated to this concept—the Antitrust Compliance Network. As the group grew globally we coordinated work in this area, shared drafts and ideas, and reported on developments around the world. Over time we started to see attitudes change. We were helped enormously by the fact that enforcers in other areas of the law were already doing this by following the Sentencing Guidelines model of offering a practical standard for compliance programs and recognizing companies that tried to implement effective compliance programs.

I had done work in the anti-corruption field and had worked with people in the Criminal Division of DOJ and with the SEC. I had been part of the SEC's first internal workshop for enforcers on the FCPA. I had even been a witness for the United States when the OECD's Working Group on Bribery did a review of US compliance with the Anti-Bribery Convention. I had explained the role of compliance programs in fighting corruption. I constantly

drew on this model, as well as working with more advanced competition law enforcement agencies like the Canadian Competition Bureau.

Initially the Antitrust Division was the only prosecuting division in the US Department of Justice that ignored compliance programs. But eventually they came around. Other antitrust agencies at various points around the world also opted for a more rational approach and recognized compliance programs. Can I take credit for this, or can our email group? Well, we did win a special award from Concurrences for our work. I certainly cannot say we changed the world. But we were at least very close to the action. Now we still have Europe's DG Comp that is stuck in a rut and on the record in favor of simply ignoring compliance diligence. Will they eventually come around? Hopefully they will and we keep working on it. If we want compliance programs to become more effective we need government to move things forward by recognizing effective compliance programs.

**Snell:** What was the first compliance book you wrote?

**Murphy:** The first compliance book I wrote was Sigler & Murphy, *Interactive Corporate Compliance: An Alternative to Regulatory Compulsion* (Greenwood Press, 1988). My college mentor, Jay Sigler, co-authored the book with me and this also happened to be the first book written on the field of compliance and ethics. There had been some guides written about compliance in specific legal areas, but no one had written about it as a field on its own. As a matter of fact, Jay and I got this out three years before the Sentencing Commission published its Guidelines.

**Snell:** What do you think of compliance certifications?

**Murphy:** There is a major distinction here when talking about "certification." So let's put aside certification of *programs* and talk about certification of *professionals*. I have an insider's view of this, because I was involved in HCCA's and SCCE's certification programs from day one. I know the intense work that went into developing those programs, how extraordinarily difficult it is to write acceptable examination questions, and what lengths HCCA and SCCE went to in order to do this the right way. For example, I see others offering "certifications" that have a tie-in to their own revenue-producing training. We learned right at the beginning that this is not actually considered ethical in the certification field, and that people need to be free to select their own sources for education. So SCCE and HCCA offer plenty of training, but there is absolutely no requirement that anyone take training from HCCA or SCCE to sit for the exam or to be certified. I think certification of compliance professionals is a good step. It communicates to the world that those who are certified are committed to this field, and are not doing it as just another job until something else comes along.

**Snell:** Tell us about some of your international efforts to help encourage the implementation of compliance programs.

**Murphy:** When I was in-house I traveled the world on mergers and acquisitions work, and on ensuring compliance with all our acquisitions and international partners. So from the beginning I could see this was a universal issue. For a couple years I traveled for the US Department of Commerce promoting compliance programs to fight corruption. This involved Botswana (one of my favorite places), Ethiopia, India and Malaysia. So when SCCE came along I was right there pushing for international development of the field. Lucky for me, Roy was all in and willing to take the risks. There are too many stories to tell, but I remember our first overseas academy in Zurich, and hearing

Kristy Grant-Hart speak in London. SCCE is much better and dynamic because it focused on being international. Early on I made friends with Shin Jae Kim in Brazil and we worked together for years to build recognition of compliance there. Through Professor Danny Sokol I met Javier Tapia, then working for the Chilean competition agency, and we then worked together to promote antitrust compliance in Chile.

**Snell:** You spent a lot of time helping the Health Care Compliance Association and the Society of Corporate Compliance and Ethics. What did they do that was more effective than others? What do you think they could have done differently?

**Murphy:** I had looked carefully at the EOA, which was then the top compliance organization in the US. EOA was a closed shop. If you did not work in-house you were treated as basically unworthy. If you were a consultant, for example, they would take your money to exhibit at their programs, but otherwise you were not welcome. When Australia began its journey in the compliance and ethics world, I watched the model they used. The Australian organization, then called the Association of Compliance Professionals of Australia, followed the open-door policy. If you were interested in the field then you were welcome. I saw this operate very well, and knew that was the right model. When I got involved in HCCA and then SCCE I saw that they used the open-door approach, and knew this was the right way to help strengthen the field.

SCCE was not afraid to make mistakes. They followed the approach I believed in - that the only way to avoid mistakes was to do nothing. So go ahead and try. Continue what works, and learn from what doesn't. SCCE was more entrepreneurial than many for-profit companies I knew of. It saw the opportunities and was not afraid to pursue them.

As for the future, SCCE should go after the major sub-areas that are in the compliance space. The potential field is much larger than SCCE has reached, both globally and in terms of the different compliance subject areas. It should go after both more aggressively. SCCE had great success in Brazil, but did not convert that same formula to other areas. (Shin Jae Kim was the champion there.) There could also do more outreach to other groups, especially local and national compliance groups in other countries. SCCE may be the largest cross-industry group, but it should really be ten times its current size. There are enormous opportunities in other countries, such as India and France, but we have not ridden that wave.

There are also entire compliance subject areas we have not reached or barely touched, such as environmental, workplace safety, securities law, and anti-money laundering. This is not to say it would be easy—difficult, after all, is not a synonym for impossible. But it seems like we are not bringing our full attention and imagination to these areas. Understand me here: This is not criticism. What we have done is outstanding and more than others have done or even tried. We worked hard and took some chances but our vision should be of a membership over 100,000. Focus, determination and persistence could be directed to this growth. It is there for whoever has the drive, will take the risks, and will focus on what are the best ways to get there.

**Snell:** Environmental, Social and Governance programs are all the rage and, in fact, we are starting a regular feature on ESG with this issue of the Journal. Some think compliance should be involved in ESG. What are your thoughts about ESG's connection to compliance and ethics?

Continued on page 71

Regina K. Alexander

# Focus Arrangements Transaction Reviews: The Curling of Compliance Work Plans?

**Regina K. Alexander, FACHE, CHC**, serves as Director of Independent Review Organization Services at BerryDunn, a full-service assurance, advisory, and consulting firm headquartered in Portland, Maine. Regina supports clients under Corporate Integrity Agreements with the HHS OIG in meeting their specific compliance obligations associated with CIA terms, including Claims and Arrangements reviews. Her areas of consulting expertise include HIPAA, Cures, No Surprises, Stark and AKS operational compliance, revenue integrity, Medicare and Medicaid payment policy.

Regina is a board-certified fellow (FACHE) in healthcare management through the American College of Healthcare Executives. She also maintains certification in healthcare compliance (CHC) through HCCA. Regina holds an MBA from The George Washington University and is an associate faculty member in the College of Health Professions at the University of Phoenix.

Originating in 16th century, Scotland and popular primarily in northern hemisphere countries where Scots have emigrated, curling is one of those winter sports the majority of the general public do not think about between quadrennial Olympic Games.[1] Often referred to as chess or shuffleboard on ice, success in the team sport of curling requires mastering skills, rules, and terminology that aren't intuitive.

Similarly, for healthcare compliance professionals, establishing a scalable and effective system for tracking and periodically auditing focus arrangement transactions can seem akin to curling for the uninitiated. The legalistic terminology, combined with lack of transparency when sensitive business details such as physician remuneration are involved, often translates into lack of awareness even at the compliance officer level regarding their own organization's risk level. Responsibility for arrangements compliance, if formally assigned at all, is often siloed within the internal legal department, or delegated to outside counsel. Whereas navigating the legal implications of Anti-Kickback Statutes (AKS) and Stark should absolutely be reserved for health law attorneys with AKS expertise, overseeing operational compliance with AKS and Stark should ideally be a team sport.

## Throwing Stones Toward Houses

Any agreement between a health care entity and any actual or potential source of health care business or referrals to the entity, or any actual or potential recipient of health care business or referrals from the entity that may implicate AKS, or Stark is considered a focus arrangement. Health care entities with agreements implicating AKS or Stark should ideally also have some form of an Arrangements Compliance Program to mitigate the organization's risk exposure.[2] For compliance officers with a lower degree of familiarity with AKS and

Stark, or with under-resourced programs, the prospect of adding arrangements oversight or transactions auditing to an already long list of work plan items seems aspirational at best.

Olympic curling is played on an ice surface called a sheet, roughly the size of a hockey rink. At opposite ends of the sheet are what in curling parlance are referred to as "houses," 12 ft. round bullseyes with centers called buttons.[3] During each round or "end," the curling teams take turns aiming and sweeping carefully to guide their 42 pound stones at the houses. Unlike other ice sports like hockey where a smooth surface is preferred, prior to the start of matches, the ice is sprinkled to create a surface with the friction necessary to make the rocks curl.

Fortunately, if an organization's internal compliance risk assessment has identified AKS and Stark compliance is a significant risk, implementing an appropriately scaled program that includes periodic transactions level review doesn't require throwing stones or creating friction with internal stakeholders. Nor does it require a compliance officer to become an expert in conducting or designing Arrangements Reviews. The publicly available Office of Inspector General (OIG) for the Department of Health and Human Services (HHS) Corporate Integrity Agreement (CIA) documents with Arrangements Review obligations provide detailed expectations for how Independent Review Organizations (IROs) are expected to conduct Arrangements Systems and Transactions Reviews.[4]

IROs typically employ a team of former compliance officers, attorneys with AKS expertise, as well as valuation experts. Healthcare organizations of any size or specialty can leverage the same publicly available instructions within CIAs that IROs use. With planning, creativity and perhaps some initial outside coaching, recruiting a team of internal stakeholders to participate in designing tracking systems and assisting compliance with conducting periodic reviews makes measuring effectiveness more feasible for resource constrained programs.

## On the Broom

The most desirable curling shot results in a stone that leaves the thrower's hand on the target line from the hack to the broom. Olympic caliber curlers make this shot look easy. Finding a CIA document with an Arrangements Review appendix is not easy because the HHS-OIG CIA Web site is organized alphabetically by CIA party name. Luckily, with the exception of vendors, the content of CIAs with Arrangement Transaction Review requirement does not substantively vary by organization type or specialty. Recent CIAs with Arrangements Review obligations are listed in Figure 1.

Whereas the body of the CIA provides a significant trove of detail and citations, including sections describing *Focus Arrangements Procedures* and *Focus Arrangements Requirements* providing salient guidance for developing a program, more practical tips for structuring a transactions review are found in Appendix B (or C).[5] Figure 2 includes each of the elements an IRO is required to assess compliance of randomly selected transactions. Given the objective of auditing transactions is to measure internal compliance with the systems, processes, policies, and procedures an organization has formally established, if an element such as maintaining service and activity logs, is not applicable to any Focus Arrangement types the organization engages in, for the purposes of fulfilling a compliance work plan item, omitting non-applicable review items is advisable.

## Mind the Hog Line

Similar to a foul line in baseball, in curling the placement of a stone within the boundaries of the hog line determines whether a stone is in play. Likewise, CIA documents provide definitions that can

*Figure 1: CIAs with Arrangements Review Obligations*

| Organization | Type/Specialty | Effective Date |
|---|---|---|
| Arthrex Inc. | Vendor/Surgical Devices | 11/8/2021 |
| Flower Mound Hospital Partners, LLC | Provider/Acute Care Hospital | 11/30/2021 |
| UCI Medical Affiliates of South Carolina, Inc. | Provider/Urgent Care Center | 4/6/2021 |
| Southwest Orthopaedic Specialists, PLLC | Provider/Physician Specialty | 7/7/2020 |
| Oklahoma Center for Orthopaedic and Multi-Specialty Surgery | Provider/Surgery Center | 7/7/2020 |
| Vascular Access Centers, LP | Provider/ Specialty Outpatient | 10/9/2018 |
| Greenway Health, LLC | Vendor/Health IT Software | 2/5/2019 |
| Sweet Dreams Nurse Anesthesia, LLC | Provider/Anesthesia Services | 8/5/2016 |
| Integrated Oncology Network, LLC | Provider/Outpatient Oncology & IMRT | 3/19/2018 |
| Homebound Healthcare Inc. | Provider/Home Health & Hospice | 10/11/2016 |

*Figure 2: Sample Arrangements Transaction Review Template*

| | | | |
|---|---|---|---|
| **Transaction Type** | | **Reviewer Initials** | |
| **Transaction Date** | | **Date Reviewed** | |
| **Date of Original Contract/Agreement** | | **Findings/Observations? [Y/N]** | |
| **Customer/Parties to Agreement** | | **Final Review Status** | |
| **Transaction Value** | | **Recommendation(s) Y/N?** | |
| **Review Step** | **Internal P&P Reference(s)** | **Compliant w/ P&P(s)? Y/N/NA** | **Observations/Notes** |
| Documentation provided indicates selected transaction details were tracked in Organization's 'centralized system'? | | | |
| Documentation provided includes parties, covered person(s), terms, performance details as applicable to the Focus Arrangement and transaction type. | | | |
| Transaction was reviewed by legal or met criteria to bypass review per applicable Organization policy/procedure for Arrangement type? | | | |
| Transaction was reviewed by business units or met criteria to bypass review per applicable Organization policy/procedure for Arrangement type? | | | |
| Legal and Business unit approvals are clearly documented, including dates and identity of approver(s) and any additional approver documentation requirements were completed (if applicable per Organization policy)? | | | |
| Remuneration associated with transaction is in compliance with FMV established per Organization policy/procedure for Focus Arrangement type? | | | |
| Business need/rationale is documented in transaction record? | | | |
| Business need/rationale is in alignment with applicable Organization policy/procedure for Focus Arrangement type? | | | |
| If Focus Arrangement type requires a service/activity log, log is complete and compliant with applicable Organization policy/procedure? | | | |
| Organization/Parties to Arrangement authenticated agreement date is prior to date remuneration released/received for selected transaction [if applicable to Type] | | | |
| Record of transaction supports review/approvals occurred prior to date remuneration released/received. | | | |

be applied to inform and customize the scope of an AKS compliance program, as well as provide a guide to constructing a simple, credible transactions review to assess Arrangements Program effectiveness. How an organization defines these key ideas also establishes the foundation for creating policies and procedures, as well as an AKS friendly, sustainable contract management process that includes assessing risks of new agreements and determining which types of arrangements transactions the compliance team should consider auditing (if any!). Involving an attorney with AKS expertise to work with compliance during the initial phase of designing the Arrangements Compliance Program is arguably non-negotiable; however, performing the deliberate exercise of defining terms such Arrangements, Focus Arrangements, and Covered Persons within the unique business and operational context of the organization is crucial to establishing the boundaries and stakeholders of an internal program or transactions review.

## Endnotes

1. *https://www.rulesofsport.com/sports/curling.html.*
2. Focus Arrangements CIAs: A Good Model for Stark/Anti-kickback Statute Compliance Programs? *Journal of Health Care Compliance*, 21(5), 23–42, September–October 2019.
3. *https://thegrandslamofcurling.com/beginners-guide-to-the-rules-of-olympic-curling/*.
4. *https://oig.hhs.gov/compliance/corporate-integrity-agreements/cia-documents.asp*.
5. *https://oig.hhs.gov/compliance/corporate-integrity-agreements/cia-documents.asphttps://oig.hhs.gov/fraud/cia/agreements/Flower_Mound_Hospital_Partners_LLC_DBA_Texas_Heatlh_Presbyterian_Hospital_Flower_Mound_11302021.pdf*.

Amy Bailey

# You Had to Be There: 10 of the Wildest Tales from a Healthcare Compliance Consultant

**Amy Bailey** has over 20 years of healthcare experience and specializes in regulatory compliance for documentation, coding, medical necessity and billing. She has extensive experience working with publicly traded healthcare companies, large hospital systems, law firms and physician group practices. Amy frequently handles routine compliance matters, as well as, assists providers subject to allegations of improper billing and also provides IRO services. Amy is certified in healthcare compliance and is also a certified coder for both physician and hospital coding, and an approved coding instructor for the American Academy of Professional Coders. She has taken many leadership roles in the industry, including serving as an Auditing and Monitoring Tools Editorial Board Member for the Healthcare Compliance Association and is also a former Regional Governor and Examination Committee Chair of the American College of Medical Coding Specialists.

As a healthcare compliance consultant for over 20 years, I have had the privilege of getting the inside view of hundreds of hospital and physician organizations. While this inside view has afforded me the opportunity to see the very best in compliance programs and operations, it has also given me a front row seat to some epic failures. I think we can all agree that we learn more from our failures than our successes and I believe there is a lot that can be learned from others' failures as well. It is in the spirit of learning and the constant striving to be better, I am sharing some of the biggest compliance disasters I have seen over my career, as well as some food for thought to help prevent your organization from making the same mistakes.

## #1- The Road to Hell Is Paved with Good Intentions

Early in my career, I was part of a team that was asked to conduct employee interviews as part of a compliance investigation into allegations of improper billing. Specifically, the allegations related to misuse of provider numbers. In the course of interviewing a billing team member, we asked the following, "tell us about a problem that you have solved". The employee then happily told us about how she eliminated all bundling denials thereby improving revenue. She "solved" the denial problem by separately reporting the services on different claims and changing the date of service by one day to avoid the bundling edits and denials. The employee truly had no idea what she had done was wrong and she was proud of how she was helping the organization.

## #2-A Single Misunderstanding Can Cause the Largest Problems

Small balance write offs are common in the healthcare industry. We have all read the guidance and have policies and procedures describing small balance adjustments. So, what happens when not everyone understands the

instructions? I was called to assist a client with an investigation and large repayment related to small balance write offs. In the process of setting up the system automation to write off uncollected small balances owed to the organization, the programmer misunderstood the instructions and programmed the system to write off all balances under $10, including credit balances. Consequently, the automation that was supposed to help efficiency, created a variety of compliance violations involving routine waiver of co-pay, improper discounts, and violations of escheat laws.

## #3-A Picture Is Worth a Thousand Words

In one of the more egregious cases I have been involved in, I was asked to provide assistance in a government investigation of a physical therapist. The investigation was initiated because the therapist often billed for therapy services in excess of 24 hours per day. As we worked to gain an understanding of the day-to-day operations, we discovered the improper practices started the moment the patients entered the facility. The seating in the waiting room was not your standard seating. Instead, the waiting room contained massage chairs and wobble chairs. The receptionist would have patients wait for their appointments in the chairs and after 8 minutes of waiting, ask them to switch chairs so everyone sat in both the massage chair and the wobble chair. The time the patients spent in the waiting room in these chairs was then billed to insurance as massage therapy and therapeutic exercise.

## #4-Don't Believe Everything You Read

In the world of electronic health records, not everything is as it appears. I was asked to assist in an internal investigation that was initiated after a hotline call alleged a physician was upcoding all of his services. During the initial phase of our audit, we reviewed a sample of encounter notes to determine whether the documentation supported the levels of service that had been assigned and in every case the answer to that question was yes. As we were concluding the matter, we reached out to the employee who had raised the complaint and advised them of our findings. The employee then provided additional information clarifying the real concern was the accuracy of the documentation itself. It was then decided we would shadow the provider in the clinic and then compare the physician's completed documentation to what we had observed. Surprise! The employee who raised the complaint was absolutely correct, the documentation in the record was not an accurate reflection of the encounter that occurred.

## #5-What a Tangled Web We Weave

We have all heard the stories of physicians performing unnecessary procedures and nurses intentionally killing patients, but we have to believe it would never happen in our organization. However, the chances are, it might. My first real experience with fraud came when I was asked to assist in a federal investigation related to overbilling of chemotherapy drugs. The case was a result of a whistleblower action suggesting the physician had billed for more chemotherapy drugs than were purchased. After pouring through years of purchase records compared to billing records, there was no denying the drug billings far exceeded the amount that had been purchased. As the defense team worked to uncover a reasonable explanation for the discrepancies, they discovered the physician had not been giving many of the patients chemotherapy at all. The physician was actually administering only saline to patients with advanced cancer but told the patients they were receiving chemotherapy and continued to bill for chemotherapy to hide the fraud.

## #6-Fact Is Stranger than Fiction

If something seems too good to be true, it probably is. I received a call from a

physician in a group I had been assisting. He wanted to discuss a "hypothetical" situation. The conversation started something like, "hey, if a PA or NP is in the OR beside me and doing surgery while I am in a different OR doing surgery at the same time and I am available to answer questions, is it ok if I sign their operative note and the surgery be billed under my provider number"? Unfortunately, the physician had been told this practice was not only ok, but that it was encouraged to maximum revenues. A review of the physician OR schedules painted a grim picture. The physicians were routinely double booked for surgeries. While the physicians performed the more complicated procedures, the NPs and PAs performed the simple procedures. However, all surgeries listed the physician as the surgeon, the NP or PA as the assistant and the reports were signed by the physician and billed using their provider number.

## #7-Money and Greed Are a Dangerous Combo

We operate in an environment that rewards our high-volume producers. We congratulate the ones who do the most. We hold those top performers out as the gold standard of what everyone else should be trying to achieve. But what if those extraordinary achievements are just a house of cards waiting to topple down? I was contacted by general counsel to assist in a matter involving a government investigation of their top cardiologist. The cardiologist had been performing and billing significantly more stent procedures than any other cardiologist in the area. In reviewing the cardiologist's notes, as well as his documented interpretations of cardiac cath and nuclear medicine study findings, the patients all had high grade blockages in vessels where stenting would be appropriate. As the investigation progressed, the government alleged the notes were actually falsified and the services provided were not medically necessary. An independent review of the films and images by an expert cardiologist supported the government's findings. The physician had been making false statements in his documentation to make it appear the services he was performing were appropriate. He did so counting on the fact that someone would not independently verify the images.

## #8-Ask No Questions, I'll Tell You No Lies

One of the biggest problems we face in healthcare compliance is people don't know what they don't know and often what seems like a straightforward problem on the surface devolves into a complicated mess of issues. I was contacted to assist with quantifying a "straightforward" billing issue related to hyperbaric oxygen (HBO) treatments. An employee raised a concern regarding overbilling of units. In speaking with a number of employees, there were no other concerns raised. However, in the course of reviewing records, a number of additional issues came to light. The ordering physician's records, often conflicted with the facility's HBO records in terms of diagnosis, prior therapy/treatments, number of dives ordered, etc. The facility staff was unaware of the conflicts because they did not request physician progress notes as a routine course of business to verify/validate the patients met medical necessity, as well as coverage, requirements prior to treatment.

## #9-Knowing Where You Came From May Give You an Idea of Where You Are Headed

Tracking and monitoring physician referrals is not a new concept for most compliance departments. However, what if your new patients are coming from somewhere other than a physician referral? Is compliance tracking that? Do you even have a mechanism in place for your physician practices to track and report that

up to compliance? I was engaged to conduct a routine compliance audit. The practice manager was new and sent the entire patient file, including the new patient paperwork, for each of the patients that had been selected for review. Typically, in the course of conducting a documentation and coding audit, I would not see the patient's registration paperwork. However, in this case, I had to page through it to get to the progress notes I was asked to review. Something interesting caught my attention. Every patient answered the "how did you hear about us" question in the same way, Facebook. That was certainly unusual, so I took a moment to search for the practice on Facebook. What I found were multiple posts advertising free visits and consultations as well as multiple posts containing misinformation about Medicare coverage of certain procedures. Based on the concerning nature of the posts, I reached out to legal counsel. Further investigation discovered that the free consultations were not even performed by licensed medical professionals and the same unlicensed staff were recommending extensive invasive procedures and expensive medical equipment for every single patient.

## #10-Necessity Is the Mother of Invention

There once was a physician who had so many locums he didn't know what to do. My very first project as a consultant involved a physician who had been prosecuted for fraud and abuse, served time and was excluded. Upon being released from prison, the physician concocted an elaborate new scheme to bring in locum tenen physicians on a rotating basis. What the unsuspecting locums did not know was that the physician intended to permanently borrow their provider numbers as a means to set up continued and excessive billing of services to federal payers. Because the physician was so aberrant in the volumes of services he was billing, his practice ended up under investigation again. He was convicted of multiple crimes and sentenced to federal prison again.

> **It is good to learn from your mistakes. It is better to learn from other people's mistakes**
>
> -Warren Buffet

I have learned that most organizations and most people are doing the best they can with what they have. Compliance departments are notoriously understaffed and underfunded. In most cases, compliance violations are genuinely mistakes rather than intentional fraud. However, as a compliance professional, you have to be prepared for both. How do you maximize the effectiveness of your efforts while operating with limited resources?

First and foremost, I think we need to acknowledge and accept that while traditional auditing methods have some value, they provided limited insight. As rapidly as healthcare is changing and the pressure to quickly identify problems and mitigate them is increasing, we have to evolve as compliance professionals. The million-dollar question is how?

In each of the cases above, we have the benefit of hindsight. It is easy to see what could have been done to identify the issues sooner. I guarantee you that each of those issues exist today and are happening in multiple organizations, possibly, likely, even yours. Let's explore some practical tips and ideas that can increase your chances of having a highly effective compliance program.

**Be visible!** The face of compliance should be more than a hotline number on a poster on a wall. I encourage you to get out of your office and into the departments and practices you oversee. As people start seeing you as a real person and the name and face of compliance, they are going to be more likely to come to you when it matters. This approach also gives

Continued on page 71

LORI A. FOLEY

# Physician Practice Acquisition: Operational Due Diligence

**Lori A. Foley** leads PYA's compliance service line and is a member of PYA's Compensation Valuation Physician Service teams. She combines industry experience in managing multiple hospital-owned practices with over two decades of consulting experience advising physicians, and organizations affiliating with physicians, in the areas of compliance, compensation, strategic planning, operational and financial improvement, and affiliation structures. Recently, Lori has been immersed in assisting organizations with understanding the volume-to-value transition, population health management, and deployment of chronic care, transitional care management, and remote patient monitoring structures so providers can use existing CMS-funded mechanisms to learn survival skills for value-based reimbursement.

It is well known that the acquisition of medical practices is happening at a rapid pace by hospitals, private equity funds, and practice consolidators. When contemplating an acquisition, most are familiar with the usual due diligence components including legal, coding and documentation, and financial. Often overlooked, however, is operational due diligence—which includes compliance components - that can at a minimum be insightful and at its best can help avoid unnecessary risk. Instead of relying on an onboarding or integration team to uncover any number of regulatory, operational, and financial hurdles, many items on a "Day 1 To-Do List" can actually be populated through operational due diligence before the transaction ever closes.

Areas where risk can lurk within a medical practice include the following:

- Revenue Cycle Processes—
  - *Filing "Insurance Only"*—Payer contracts generally require the provider to bill patients for their copayment, deductible, and applicable coinsurance. Submitting claims for insurance payment without pursuing patient responsible balances violates those agreements and may impact "usual and customary" reimbursement calculations. Additionally, if done for patients with Medicare or Medicaid, this practice can be viewed as an inducement for patients to use the provider for clinical services which implicates the civil monetary penalties law and violates antikickback statutes.
  - *Failing to refund overpayments*—Governmental payers require providers to repay overpayments within 60 days. Some practices fail to monitor their credit balances to identify and address overpayments in a timely manner, relying solely on the payers to identify and recoup these funds. This can result in an accumulation of credit balances with amounts due to government payers that are older than 60 days.
  - *Unclaimed Refunds*—Many practices are unaware that they must follow state escheat laws and report unclaimed property. While state laws vary,

unclaimed property may include refunds due to patients who can't be found through reasonable means. In these instances, the practice must remit the funds to the state rather retaining them.

- OSHA Requirements
  - ❏ *Failure to provide OSHA training*—Practices are required to train employees on key OSHA regulations including the following standards: Bloodborne Pathogens, Emergency Action Plan, Fire Safety, Hazard Communication and Exit Plan. This includes new employees who must be trained within 10 days of hire and all employees who must receive refresher training and have the ability to ask questions each year.
  - ❏ *Failure to offer Hepatitis B vaccinations*—The Bloodborne Pathogens Standard requires healthcare providers to offer the hepatitis B vaccination to any employee who is reasonably anticipated to have exposure to blood or other potentially infectious materials. This offer must occur within 10 days of the employee's start date and must be no-cost to the employee.
- HIPAA
  - ❏ *Failure to post Notice of Privacy Practices (NPP)*—HIPAA's Privacy Standard requires that practices post their NPP in the waiting room in a conspicuous place. It also requires the NPP to be posted on the practice's Web site should one exist.
  - ❏ *Failure to perform a HIPAA Security Risk Assessment (HSRA)*—HIPAA's Security Standard requires covered entities to perform a HSRA to evaluate compliance with HIPAA's administrative, physical, and technical safeguard requirements.

While the items described above seldom represent "walk away" risk, insight acquired through operational due diligence allows the buyer the opportunity to focus immediate attention on areas needing remediation as it sets about fully integrating the acquired practice into its own operations.

Gary N. Jones

# Can Your Compliance Program Be the Key to a Successful Merger?

**Gary Jones** has been an attorney for over 35 years and has spent most of the last 25 years focusing on the needs of facilities and agencies in the human services field. He obtained his bachelor's degree from the University of Missouri in 1982, and his Juris Doctorate from the University of Missouri-Kansas City, School of Law in 1985. Gary holds the CHC and CHPC certifications. In addition to an active law practice, he founded MCA to help providers through the maze of compliance regulations that seems to become more complicated every year so they can do what they do best, take care of people. He is the author of "Do The Right Thing—a road map to building an effective compliance program."

For many reasons, there has been a steady increase of mergers in health care over the last few years. The pandemic has placed a renewed emphasis on just how fragile it can be to be a health care provider, especially a smaller provider. Without the critical mass needed to survive both a shutdown of the economy, and the extreme staffing crisis experienced over the last two years, many providers have sought out larger providers as merger partners in an effort to continue to provide critical health care services. Many of the recent mergers have happened quickly, almost as a lifeline to an organization on its last breath. It has not been unusual for a merger where the target organization is much smaller than the acquiring organization that the merger is completed in a matter of weeks as opposed to a matter of months. Whether the merger process happens quickly, or takes several months, an often forgotten or overlooked component of a merger is the blending of cultures of the involved organizations.

## Overview of Organizational Culture

Culture can be defined many ways, but they all come down to an established way of doing things. Each of us has an individual culture based on factors such as where we live, how we were raised, or even the food we like. (There is most certainly a culture based on BBQ!). Organizations also have cultures and a good definition is as follows: the shared set of attitudes, values, goals, and practices that characterizes an institution or organization.[1] In simple terms, an organization's culture is defined by "this is how we do things around here."

Cultures, individual or organizational, don't happen overnight. Rather, they can take years to develop. People will cling to, and defend, their culture, often to their detriment. But why do people, and organizations, hang on to their culture so tightly? Culture provides identity, and the loss of culture means a loss of our identity. When we know the norms, or "rules of the game" so to speak, we are much more comfortable. When the rules change, or in the situation of a merger,

a whole new set of rules apply, our level of comfort sinks. When that happens, it is natural for us to cling to the known, what gives us comfort, as opposed to embracing a whole new way of doing things.

While it does happen that two or more organizations come together to form a completely new organization, most mergers involve two organizations where one of the two is the surviving organization, and the operations, employees and patients/clients of the other are joined into the surviving organization. There are Letters of Intent, Merger Agreements, sometimes months of due diligence work, and a great deal of legal work that goes into successfully merging two organizations. But, once the legal work is done, what really happens in a merger? The employees of the acquired organization are on-boarded into the new company, given a new name badge and t-shirt, and often go right back to work doing what they were doing before the merger. Taking care of the same people, fixing the same equipment, cleaning the same rooms, etc.

But it often doesn't take long for the buzz of a merger to calm down and then the realization hits that some things are different. Titles may change; administrative procedures are different; there are new rules to be followed. Soon things begin to feel very different, and different isn't always good. No one likes to have anything done "to" them, and mergers tend to lend themselves to that very feeling by many of the people impacted by the merger, those front line employees and middle managers that work each day to carry out the mission of the organization, but who had no say in the decision to merge.

The legal documents, the due diligence, and all the work that takes place in the C-suite are actually the easy part of a merger. Where the rubber really meets the road is how things are handled after the merger has been finalized, and the t-shirts with the new logo have been given to all the "new members of the family" so to speak. Without deliberate effort to merge, not only the operations of the organizations, but also the respective cultures, disaster can strike in the form of frustration, a sense of being out of control by many in the organization, and eventually, loss of the talent that made the companies what they were before the merger occurred.

A prime example of a merger that failed due almost exclusively to the clashing of organizational cultures is the 1998 merger of Daimler-Benz and Chrysler. This particular merger has been studied and analyzed, maybe more than any other failed merger, and is an example of what happens when differences in culture are ignored. One company, Daimler-Benz, succeeded because it was very methodical in its approach to making automobiles. On the other hand, Chrysler was known as a creative environment where structure was rarely imposed. While the merger made sense on paper, the cultures of the two companies were just too different, and any effort to bring those cultures closer together proved to be too little, too late. Just 10 years later, Daimler-Benz had sold off most of the assets acquired in the merger at a loss of over $20 billion.

When deliberate effort is taken to address culture, and the impact of the respective cultures is part of the overall merger plan, there is a much higher probability of success, and retention of employees. As soon as the Merger Agreement is signed, the parties should begin the process of planning how to blend the cultures of the organizations. This plan should be on a parallel path with the plan to merge the operational aspects of the organizations.

As is stated above, people tend to cling tightly to their culture and fight any attempt to impose a new culture. If you have ever watched the process of smaller school districts consolidating, and determining in which town the elementary school will be retained, you know what

I mean! For any plan to be successful, it has to have a foothold and be able to obtain traction with those impacted by the plan. When our kids were four years old we could take the "because I said so" approach, and, quite frankly, that is how some companies go about bringing companies together in a merger, but rarely is it a successful approach. Finding something that resonates and is relevant to everyone involved; something that everyone can get behind, is the absolute best way to achieve the desired result.

## Using the Compliance Plan to Build a Shared Culture

As surprising as it may be, the compliance program is a perfect place to gain traction for the blending of cultures when two health care providers come together in a merger. We often say compliance, when you boil it down, is really just about doing the right thing. When asked, nearly every employee of either organization involved in a merger will state they are committed to doing the right thing, and it is this common goal that provides the foothold needed to begin to blend two different cultures into one new shared culture.

An evaluation of the target organization's compliance program should always be a component of the pre-merger due diligence process. Ensuring the existing compliance program addresses each of the elements of an effective compliance program allows for the development of a common language of sorts, and this language can be used to drive the blending of cultures, because, as is stated above, everyone is committed to doing the right thing. A key first step in the process is to develop a shared definition of what "the right thing" means in the day-to-day operations of the organizations. As part of the due diligence evaluation of the compliance program, it is wise to spend some time with employees who work on the front lines of the organization, as well as members of management, to determine the attitude of compliance within the organization. Armed with the knowledge of how employees view their obligations and responsibilities under the compliance program, the acquiring company can identify the areas where the two organizations share values. Those shared values become the building blocks of the new organizational culture. The more common ground there is, the easier it is for employees to transition into the new company. If they feel the surviving organization is ethically aligned with their value system, employees of the acquired organization will trust the new procedures, new leadership and even the new direction under which they now work.

Nearly everyone wants to be part of a team, but what does that actually mean? Maybe everyone wears the same uniform, but the more important aspect of being part of a team is the fact everyone has the same common goal. Whether it be winning the championship, or building a new culture, the power of an employee feeling like they are part of the team cannot be understated. The common goal of doing the right thing, the absolute foundation of the compliance program, can be the catalyst for development of the common language needed to drive culture.

If you are like me, as you have been reading this article you have been saying to yourself "that's all well and good Gary, but HOW do I use compliance to build a shared culture?" Just like building a house, the key is to establish a strong foundation upon which every aspect of the effort to blend cultures will stand, and that foundation is a strong commitment from leadership.

To be successful, using compliance as the catalyst to blend cultures in a merger, must be sincerely supported by leadership at all levels, but especially at the senior leadership level. Without a sincere commitment from senior leadership, which includes allocation of resources, and full public support of the effort, the

compliance program will not be effective or seen as authentic. Nothing will destroy a culture faster than compliance being seen as only a slogan and not as a way of life. If front line staff don't believe leadership is committed to compliance and the blending of cultures based on the concept of everyone doing the right thing, there is very little chance of success.

As is stated above, planning for blending of cultures by using the compliance program to establish common ground should start long before the closing date of the merger. Ideally, development of the plan involves team members from both organizations, and takes into consideration the existing culture of the respective organizations. Just as individuals have different learning styles, every organization has a way things are done within that organization; by definition, that is its culture. It is important to build the plan knowing how to use the existing culture rather than simply imposing the "new way of doing things"; again, no one likes to have anything done to them and if they feel this is what is happening, the effort will fail.

One of the first steps in the plan is to develop a strong brand for the compliance program; a brand that says we are all committed to doing the right thing. A fun logo (fun does not equal cutesy!), or a catch phrase that people can remember is a great way to establish the compliance brand. A phrase I like to use is "Employees doing the Right Thing, the Right Way, at the Right Time."© A catch phrase that clearly sets forth the expectations, and the shared values, of the compliance program is a great way to bring everyone to the same level. There are many ways to build and promote the compliance brand such as posters, give-a-ways, contests, etc. The goal is to show that everyone is committed to doing the right thing, and the compliance program is more than just "catching people doing something wrong." Rather, the commitment to doing the right thing is part of the fabric of the merged organizations.

Early in the planning process it is essential to identify those employees who will be the internal advocates of the effort, the compliance champions if you will. These are the front line employees and middle managers that staff will look to in order to determine if everything is okay. Many organizations, especially large providers, can feel somewhat impersonal for front line employees, and when big news hits like finding out the company is being acquired or merged into another organization, it can be scary for these folks. Front line staff may have never met the CEO; for them, the face of the organization is their supervisor. How the supervisor responds when staff want to know if everything is okay will make or break the effort to blend cultures. By enlisting supervisors or middle managers, from both organizations, in the effort to use compliance to blend cultures, there is a system of internal advocates who can assure staff that while they may wear a new logo on their shirt, everyone is committed to doing the right thing and providing the highest quality of care to the people served by the organization. To achieve buy-in, it is important for employees to see people they know and trust on board and engaged in the effort. This article has spent a lot of time focusing on the organization being acquired, but these principles apply to the acquiring organization as well. The blending of cultures impacts everyone.

## Conclusion

The blending of cultures takes time and deliberate effort. An important factor in the success of using the compliance program to establish common ground is to keep the big picture in mind. The goal is to blend cultures not impose one organization's culture in place of another organization's culture. For the most part, people work

Continued on page 72

Jenny O'Brien

# What Is It and Why Should You Care?

**Jenny O'Brien, JD, MS, CHC**, is President of BlackBridge Advisors, advising organizations on regulatory, risk, governance, and ESG issues. Most recently, Jenny was the UnitedHealthcare (UHC) Chief Compliance Officer where she was a member of the Executive Leadership Team and accountable for developing a national compliance strategy across all products. Jenny serves on the Board of Bon Secours Mercy Health as Chair of the Audit & Compliance Committee, sits on the Board of St. Charles Health System and is a Board member and Past President of HCCA/SCCE. She is certified in Healthcare Compliance (CHC) & Privacy (CHPC).

When I was recently asked if I'd write a six piece series over the next 12 months on the topic of ESG (Environmental, Social, Governance) I probably should have declined since I am definitely not one of the so-called ESG industry experts. However, when the "ask" was clarified to share my experiences and expertise as a compliance professional and connect the dots with what's occurring within ESG, I was hooked and said challenge accepted.

As a compliance professional there is always something new to learn, and for the past year I have been jumping on ESG virtual conferences, reading articles and joining discussion groups in an effort to absorb viewpoints of those recognized as "experts in the business." I knew I needed to educate myself so I could better respond to questions I was getting as to how ESG risks related to the work of compliance teams as well as what role compliance professionals would play and how they could support the emerging focus in this area. To do this it is important to understand, first of all, what is ESG and, secondly, why should I and many other compliance professionals care.

So for those just joining the discussion, ESG in its simplest terms means:

- **E = Environmental:** Encompasses initiatives that determine a company's impact on the environment (*e.g.*, climate, water-related issues)
- **S = Social:** Includes people-related issues that impact employees, customers, suppliers (*e.g.*, diversity and inclusion, social justice)
- **G = Governance:** Oversight of these areas (*e.g.*, board composition, executive compensation)

In looking for the answer of why it's important to have ESG on your radar, the answer is the same for any evolving risk area, it's our job. The most effective compliance programs are always looking around the corner for the next area to leverage our program and provide strategic direction to support emerging risks. We are already heavily involved in the governance bucket and as you start viewing ESG in a broader lens you may

realize you are already measuring a number of key metrics that are included within the other two buckets, such as diversity and inclusion, culture and engagement and response to the COVID-19 pandemic.

If you aren't already on this path I hope you join my journey. As with all new areas I set out to explore, I'm energized and intrigued by the discussion but am also finding I have more questions rather than being satisfied with answers. Let the learning continue and in the next article we will move beyond why you should care to discuss whether and what type of program may be appropriate for your organization.

Joshua M. Robbins / Ryan Stasell

# Increasing EKRA Enforcement May Expose Gaps in the Statute

**Joshua M. Robbins** is a Shareholder and Co-Chair of Buchalter's White Collar and Investigations Practice in the firm's Orange County office.

**Ryan Stasell** is an Attorney and member of Buchalter's Litigation and White Collar & Investigations practice groups in the firm's Orange County office.

Since it was enacted in 2018, the Enforcing Kickbacks in Recovery Act (EKRA) has marked a major expansion of the federal anti-kickback enforcement regime in health care. While the Anti-Kickback Statute (AKS) had for years prohibited payments for referrals of patients covered by Medicare and other federal health insurance programs, EKRA for the first time made such payments illegal for certain referrals involving patients with commercial insurance or other non-federal coverage. Addiction treatment providers, sober living homes, and diagnostic laboratories quickly found themselves in the crosshairs.

But for all the attention EKRA garnered at first, there have been fairly few prosecutions under it, and thus few court decisions interpreting it. That is likely to change soon, as the Department of Justice makes good on its promises to ramp up enforcement of the law, and whistleblowers seek to incorporate it into *qui tam* and retaliation claims.

The ensuing litigation, however, may reveal what appear to be holes in EKRA's text and design. That is perhaps unsurprising: as one congressman observed, EKRA "did not go through regular order," "was not properly vetted," and "was added at the very last minute," raising concerns that its language "does not do what we think it does," and "may have unintended consequences."[1] When a new criminal statute is passed in a hurry, those consequences can be significant.

In particular, the law's text appears to leave room for covered providers to engage in certain payment practices often assumed to be banned, and may provide defenses to those who have already done so. First, as already found by one court, EKRA's rule barring payment for referrals may not affect value- or volume-based payments to sales and marketing staff who solicit patient referral sources such as hospitals or primary-care practices, rather than recruiting patients themselves. Second, and perhaps more importantly, by directly importing from the AKS regulations a "safe harbor" that was designed for the AKS federal

program regime, EKRA may even allow for value- or volume-based payments for *direct* recruitment of patients, provided it is done under a properly-designed written contract.

## Gap One: Payment for Indirect Referrals

One potential EKRA gap, which has already been acknowledged by at least one federal court, may allow labs and addiction treatment providers to pay sales or marketing staff on a patient volume or value basis, provided the staff interact only with referral sources such as hospitals, rather than directly with patients, and the referral sources themselves are not paid.

18 U.S.C. § 220(a) contains EKRA's basic prohibitions. Subsection (a)(2), in particular, makes it a crime to knowingly and willfully "pay[] or offer[] any remuneration (including any kickback, bribe, or rebate) directly or indirectly . . . (A) **to induce a referral of an individual** to a recovery home, clinical treatment facility, or laboratory; or (B) in exchange for an individual using the services of that recovery home, clinical treatment facility, or laboratory."

Like other health care providers, labs and addiction treatment facilities may employ or contract with marketers to build relationships with potential patient referral sources, such as hospitals, clinics, or medical practice groups. They may also seek to incentivize such marketers by paying them based on the number or value of patient referrals that result from their work. Would that violate EKRA subsection (a)(2)? A federal court has said no.

In *S&G Labs Hawaii, LLC v. Graves*,[2] a diagnostic lab employed a marketer in such a role, and paid him in part based on the net profits from resulting patient referrals. When the marketer later sued the lab for breach of contract, the lab responded that the contract had become illegal when EKRA was enacted, because it entailed payment to induce referrals.

The court disagreed. It found that the lab's payments to the marketer were not made "to induce the referral of an individual" to the lab, as the marketer was involved only in connecting the *referral sources*—*e.g.*, the hospitals—with the lab, and did not directly recruit the "individual" patients who were to receive treatment. Thus, the court found, EKRA subsection (a)(2)(A) did not apply. The court also found subsection (a)(2)(B) inapplicable because the lab was not paying the marketer for his own use of the lab's services, thus taking a narrow reading of that provision as covering only cases where patients themselves are paid kickbacks.

Though not addressed in *S&G Labs*, One might object that subsection (a)(2) includes the phrase "directly or indirectly," and that the marketer was effectively being paid for indirect referrals. But the phrase at issue is more clearly read to modify the earlier terms "pays or offers remuneration," rather than "to induce a referral," meaning that payment made to A to induce referral of B, with the intent that B will refer C (the patient) is not covered.

While it is too soon to know whether other courts will read subsection (a)(2) the same way, *S&G Labs*'s reading of the text is at least reasonable. And because EKRA is a criminal statute, any ambiguity in the language is subject to the rule of lenity, which requires that it be construed in favor of defendants.[3] Relatedly, because conviction under EKRA requires that a defendant have acted "willfully"—with awareness that he or she is acting unlawfully—*S&G Labs* may make it difficult for prosecutors to pursue cases against providers who rely on its interpretation of the law.

## Gap Two: Payment for Direct Referrals Under a Personal Services Contract

The second hole, though untested in court, may be even wider, allowing value- or

volume-based payment to sales and marketing staff even for direct patient referrals, provided they are made under an appropriate contract.

EKRA's subsection (b) sets out several circumstances in which subsection (a)'s prohibitions do not apply, akin to—and often based on—the AKS's safe harbors. One of these, § 220(b)(4), exempts a "payment made by a principal to an agent as compensation for the services of the agent under a personal services and management contract that meets the requirements of section 1001.952(d) of title 42, Code of Federal Regulations, as in effect on the date of enactment of this section." This provision thus directly incorporates the 2018 version of the AKS "personal services and management agreement" safe harbor.

That safe harbor provides that for anti-kickback purposes, the term "remuneration" does not include a payment for compensation if various criteria are met, such as that the payment is pursuant to a written contract that spells out all services to be performed, and has a term of at least one year. Another key condition, at 42 CFR 1001.952(d)(iv), is that

> The aggregate compensation paid to the agent over the term of the agreement is set in advance, is consistent with fair market value in arm's-length transactions, and is not determined in a manner that takes into account the volume or value of any referrals or business otherwise generated between the parties **for which payment may be made in whole or in part under Medicare, Medicaid, or other Federal health care programs**.

As the bold text indicates, a key restriction in the safe harbor—that payments cannot be volume- or value-based—is limited to referrals of patients covered by federal programs like Medicare. If payments are made under a contract that bases compensation on the volume or value of referrals of patients who are *not* covered by federal programs—such as patients with commercial insurance—the AKS safe harbor would still apply, assuming the other conditions are satisfied. That is not surprising for purposes of the AKS and related regulations, which were only meant to cover federal health care programs.

EKRA, of course, was meant to cover payments for referrals of commercially insured patients. But because they incorporated the AKS safe harbor language wholesale, without accounting for the bold text above, EKRA's drafters created an exception that potentially swallows the rule.

When EKRA's text is read together with that of the AKS personal services safe harbor, it would seem that a lab or addiction treatment facility could contract with a marketing company to refer privately-insured patients, pay the marketer on a per-patient basis, and still not violate EKRA. Such a contract's compensation terms would not take into account the volume or value of any referrals of federal program business, could thus satisfy the safe harbor, and would thus be exempted under EKRA subsection (b)(4).

The government may object that this was clearly not the intent of EKRA's drafters. Indeed, one of the law's co-authors, Senator Amy Klobuchar, emphasized that it was necessary precisely because while kickbacks were already illegal when federal program funds were involved, "there is no Federal law to prohibit them in private health insurance plans."[4] But courts consistently refuse to defer to asserted legislative intent when the plain text of a statute is clear and unambiguous.[5] That is particularly true for criminal statutes.[6] And again, to the extent the text is ambiguous, the rule of lenity requires that it be construed against the government, while the "willfulness" mens rea standard provides a defense to providers

who rely on a plausible reading of the statute's text.

HHS may be tempted to pursue a regulatory fix, amending 1001.952(d)(iv) to account for its incorporation into EKRA and close the hole. That would be ineffective, as the EKRA subsection (b)(4) exemption expressly incorporates the version of the safe harbor regulation "in effect on the date of enactment" of EKRA—October 24, 2018. It is also unclear that HHS would have the statutory authority to modify the regulation in order to support enforcement of EKRA, which is not the authorizing statute for 1001.952 and which does not give HHS regulatory authority.

Nor would DOJ necessarily have the power to address the issue by regulation. EKRA § 220(c) authorizes the Attorney General to promulgate regulations to "clarify" the subsection (b) exceptions. But clarification does not mean amendment, and an agency's attempt to "construe" subsection (b)(4) to grant it such power, inconsistently with the plain text, would not likely succeed.[7]

## Conclusion

For labs and addiction treatment providers considering these textual gaps, an obvious caveat remains: EKRA's youth and the scarcity of court decisions interpreting it mean there is still great risk in any system of payments for referrals. The government may well take a different view of the above points, and could conceivably persuade a court to interpret the statute more in accordance with its drafters' likely intent. Because EKRA is enforced criminally, with a potential jail sentence of up to 10 years per violation, this may be enough to discourage providers from testing these theories. But as the number of EKRA prosecutions grows, so does the possibility that courts will confront the law's textual oddities, and reiterate the importance of clarity in drafting new criminal statutes.

### Endnotes

1. 164 Cong. Rec. H9174-02, H9244 (daily ed. Sept. 28, 2018).
2. 2021 WL 4847430 (D. Hawai'i Oct. 18, 2021).
3. *United States v. Davis*, 139 S.Ct. 2319, 2333 (2019).
4. 164 Cong. Rec. S6467-02, S6473 (daily ed. Oct. 3, 2018).
5. *See, e.g., Dep't of Hous. & Urb. Dev. v. Rucker*, 535 U.S. 125, 132 (2002)("[R]eference to legislative history is inappropriate when the text of the statute is unambiguous.").
6. *See Crandon v. United States*, 494 U.S. 152, 160 (1990) ("Because construction of a criminal statute must be guided by the need for fair warning, it is rare that legislative history or statutory policies will support a construction of the statute broader than that clearly warranted by the text.").
7. *See MCI Telecommunications Corp. v. Am. Tel. & Tel. Co.*, 512 U.S. 218, 224–234 (1994) (finding that statute authorizing agency to "modify" statutory requirements did not allow it to make "basic or fundamental changes" to the law.").

## What DOJ Cares About

Continued from 10

17. Press Release, DOJ, Pharmaceutical Companies Pay Over $400 Million to Resolve Alleged False Claims Act Liability for Price-Fixing of Generic Drugs (Oct. 1, 2021), *https://www.justice.gov/opa/pr/pharmaceutical-companies-pay-over-400-million-resolve-alleged-false-claims-act-liability*.
18. *Id.*
19. *https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/*.
20. Press Release, DOJ, Justice Department's False Claims Act Settlements and Judgments Exceed $5.6 Billion in Fiscal Year 2021 (Feb. 1, 2022), *https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year.*

## Ransomware Attacks on

Continued from 16

an ongoing, pre-incident relationship with the company, providing input to the business in a non-privileged context. In such cases, it is best to have a master services agreement that provides for execution of a separate statement of work that will govern privileged activities related to any future incident investigation. And remember that it is not enough to copy counsel. Experienced incident response counsel should direct the investigation and any subsequent reports, all of which should be tightly held confidential.

There always is a premium on moderation in the creation of written, privileged work product. Historically, it was commonplace to request a comprehensive written forensic investigation report, spanning many pages. Increasingly, companies are realizing that it may not be necessary to create such reports. Often, forensic findings can be adequately communicated and processed in oral discussions. When it is necessary to prepare written reports, the company and its vendors should carefully agree on the content and scope in advance. In some cases, the company may not produce a privileged report at all and may instead choose to prepare a non-privileged factual report for communication to external stakeholders, including customers, and possibly to share with regulators.

## Hang In There

Major data security incidents are difficult and stressful. Thorough advance preparation and testing of incident response plans will make the process smoother, more effective, and less costly. Although reportable breaches will have business and reputational consequences, health care providers tend to have extremely loyal customers—your patients—who will continue to support and patronize you if you manage the process effectively, with empathy, including with respect to post-notification, patient-focused activities, such as offering call center services and credit monitoring when appropriate.

If you are ready in advance, you will get through this, and are likely to get back to normal sooner than you may think in the dark, early days of a data security incident. Plan and practice for a successful response, and you will achieve it.

### Endnotes

1. Tenable, *2020 Threat Landscape Retrospective* ("Tenable"), p. 17.
2. IBM Security/Ponemon Institute, *Cost of a Data Breach Report 2020* (IBM/Ponemon), p. 25.
3. *Id*. at 25–26.
4. Tenable, p. 18.
5. *Id*. at 40.
6. Kroll, *Ransomware Attack Trends 2020* (Kroll), p. 2.
7. 45 C.F.R. Part 164, Subpart D.
8. 45 C.F.R. § 164.402.
9. 45 C.F.R. § 164.402(2).
10. *FACT SHEET: Ransomware and HIPAA* (July 11, 2016) (*https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf*) (OCR Ransomware Guidance).
11. OCR Ransomware Guidance, pp. 5–6.
12. *Id*. at 6.
13. 985 F.3d 472 (5th Cir. 2021).
14. *Id*. at 478.

15. *E.g.*, Ariz. Rev. Stat. § 18-552(N)(2) (does not apply to a HIPAA covered entity or business associate if they comply with applicable provisions of HIPAA).
16. *E.g.*, Del. Code Ann. tit. 6 § 12B-103(b) (HIPAA covered entity that maintains procedures for a breach of security pursuant to HIPAA is deemed to be in compliance with the Delaware law if the covered entity person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs).
17. *E.g.*, Cal. Civ. Code § 1798.82(e) (a HIPAA covered entity that complies with the individual notice content requirements of the Breach Notification Rule will be deemed to have complied with the individual notice content requirements of the California law but is not exempt from any other requirements).
18. Some state laws may have exceptions to the notification requirements even if there is a breach such as a "risk of harm" exception. E.g., Ala. Code § 8-38-5(a) (notice to individual not required for security breach unless reasonably likely to cause substantial harm to the individual).
19. 45 C.F.R. § 164.404.
20. 45 C.F.R. § 164.404(b).
21. 45 C.F.R. § 164.404(c).
22. 45 C.F.R. § 164.406.
23. *Id*.
24. 78 Fed. Reg. 5566, 5648 (Jan. 25, 2013).
25. IBM/Ponemon, p. 45.
26. *See, e.g., In re Rutter's Data Sec. Breach Litig*., No. 1:20-cv-382, 2021 WL 3733137 (M.D. Pa. July 22, 2021); *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7 (D.D.C. 2021).
27. Kovel letters are named after the landmark decision in *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961), in which the court extended the protections of the attorney–client privilege to communications between an attorney and an accountant with whom the attorney had sought input in order to help advise the attorney's client.

## The No Surprises Act

Continued from 22

3. Federal Independent Dispute Resolution (IDR) Process Guidance for Certified IDR Entities, The Departments, January 2022, p. 14, available here: *https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Federal-Independent-Dispute-Resolution-Process-Guidance-for-Certified-IDR-Entities.pdf*.
4. Calendar Year 2022 Fee Guidance for the Federal Independent Dispute Resolution Process under the No Surprises Act, Technical Guidance No. 2021-01, available here: *https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Technical-Guidance-CY2022-Fee-Guidance-Federal-Independent-Dispute-Resolution-Process-NSA.pdf*.
5. Federal Independent Dispute Resolution (IDR) Process Guidance for Certified IDR Entities, The Departments, January 2022, p. 14, available here: *https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Federal-Independent-Dispute-Resolution-Process-Guidance-for-Certified-IDR-Entities.pdf*.
6. Federal Independent Dispute Resolution (IDR) Process - Guidance for Disputing Parties, The Departments, January 2022, p. 19, available here: *https://www.cms.gov/files/document/federal-independent-dispute-resolution-guidance-disputing-parties.pdf*.
7. Requirements Related to Surprise Billing; Part II Interim Final Rule with Comment Period, CMS, September 30, 2021, available here: *https://www.cms.gov/newsroom/fact-sheets/requirements-related-surprise-billing-part-ii-interim-final-rule-comment-period*.
8. *See also*, Federal Independent Dispute Resolution (IDR) Process Guidance for Certified IDR Entities, The Departments, January 2022, p. 14, available here: *https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Federal-Independent-Dispute-Resolution-Process-Guidance-for-Certified-IDR-Entities.pdf*.
9. *Texas Medical Assoc. and Adam Corley v. U.S. Dept. Health & Human Serv., et. al.,* 6:21-cv-425-JDK, 2022 WL 542879 (E.D. Tex. Feb. 23, 2022).
10. 5 U.S.C. § 706.
11. 5 U.S.C. § 553.
12. Memorandum Regarding Continuing Surprise Billing Protections for Consumers, Centers for Medicare & Medicaid Services, February 28, 2022, available here: *https://www.cms.gov/files/document/memorandum-regarding-continuing-surprise-billing-protections-consumers.pdf*.
13. List of certified independent dispute resolution entities, Centers for Medicare & Medicaid Services, available here: *https://www.cms.gov/nosurprises/Help-resolve-payment-disputes/certified-IDRE-list*.

## High Impact, Unique Risks

Continued from 42

18. The 340B Prime Vendor offers an online, on-demand "340B University" which covers the basics of 340B Program implementation. *https://www.340bpvp.com/340b-university/online-learning* (last accessed February 14, 2022).
19. 42 U.S.C. § 256b(d)(2)(B).

## For the Record

Continued from 48

**Murphy:** First, for better or worse, ESG will not stand still, and the combination of letters—"ESG"—can always be subject to change. (I personally think the "S" for social covers it all, since it is all about people—what we do and how we do it). There is definitely a role for compliance and ethics in this space. Indeed, a fair amount of ESG is or will be matters of legal requirements and thus be compliance matters. I do not think, however, that this should just be lumped into compliance and ethics. Ours is already an extremely difficult and challenging area. Too many of my peers seem to seriously underestimate how difficult this area is. We deal with preventing corporate crime. Consider that people involved in crime are often extremely creative. There is always a certain percentage of employees and agents who are sociopaths and psychopaths. We can never rest in preventing misconduct. We always need to be vigilant and improving our techniques.

We also have much to do in helping those who do want to do the right thing. We need to communicate and train these folks. We need to keep up with current means of communications to be effective. The Sentencing Guidelines contain a serious list of compliance steps. I doubt if there is a company anywhere that has fully explored what each of these steps means, and has fully mastered the art of making their program completely effective. So if we have an essential and difficult job, why are people saying "you need to do another entire job, you need to add ESG"? It is like the general counsels who tried to grab compliance and put it under their control. They were already too busy. They had neither the interest nor the time to be the general counsel and compliance & ethics officer at the same time. The same is true for us; we do not have the time, resources, or knowledge to do another full-time job. We should participate, but as a partner to someone else. We already have a big job to do and we need to do that.

**Snell**: Thank you for your time, sir.

## Best Practices

Continued from 56

you the opportunity to see what is actually going on in practice.

**Don't forget the little people!** As senior and executive leaders, we tend to communicate with other leaders and managers. In doing so however, you are robbing yourself of the opportunity to hear from some of your most valuable assets, the people who are actually doing the day-to-day work. It has been my experience, more often than not, that what the supervisors and managers think is happening, is often not what or how things are happening at all. Additionally, compliance trusts the managers and senior leaders to do the right thing when often they don't.

**Think outside the box!** The definition of insanity is doing the same thing over and over again and expecting different results. If you are holding on to the way you've always done it, your compliance program is never going to evolve or be truly effective. The Department of Justice has issued guidance on evaluating corporate compliance programs. In reading the guidance, the expectations are clear that a compliance program should be "adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees." In light of those expectations, it is important to ask yourself the following types of questions; Are your current compliance efforts designed to find only the low hanging fruit? Are your questions designed to yield specific, expected responses? Do you use the same

methodology for each of your audits? Do you unwittingly incentivize providers to game the system? Is your program stuck in 1998 still relying on the five charts per provider Compliance Guidance? If you find yourself answering yes to any of those questions, it is time to reimagine things. Start envisioning site visits and shadow audits; start thinking about outside medical necessity reviews; start thinking about the types of questions you are asking and who is answering them; start thinking about what types of data you review; that is, who is reviewing, approving and testing automated functions, who is reviewing metadata and how; start thinking about what types of documentation you typically review.

**It won't be easy!** Taking your compliance program to the next level won't be easy, but it will be worth it. Well-designed compliance programs and highly effective compliance professionals are founded on visibility, hard work, trust, and integrity. Even in today's environment where everyone is pulled in many different directions, it is possible. So, get out there and start doing compliance, who knows, maybe you will even get the opportunity to scroll Facebook ads from the comfort of a massage chair.

## Corporate Culture

Continued from 62

in health care because they want to help people. Using the commitment to doing the right thing as a way to bring two organizational cultures together plays into that deeply held value. Because the compliance program does not stand alone, but rather impacts every other aspect of the organization, the building of common ground in compliance can flow into every other department, and, before you know it, the merged organizations have built a common culture based on the foundation of doing the right thing.

### Endnote

1. *See* Merriam-Webster definition of culture at *https://merriam-webster.com/dictionary/culture* (retrieved January 25, 2022).