GAN INTEGRITY

Compliance in the Pharmaceutical Industry

Challenges and Opportunities

Table of Contents

INTRODUCTION:

Traits of Successful Programs in Pharma

Corporate compliance in the pharmaceutical industry has long been a complicated endeavor, packed with a huge range of concerns — everything from consumer privacy, to anti-corruption, to quality control, to billing fraud, and much more. All the while, compliance officers in the pharma sector also have practical operational concerns crowding onto the priority list, such as corporate mergers or data integration projects.

An effective corporate compliance program in the pharmaceutical sector, therefore, demands two traits. First, it must be robust enough that it can implement policies and procedures to address the issues facing the company. Second, it must be versatile enough to pivot to new issues quickly and efficiently amid an ever-shifting and expanding risk landscape.

What specific issues rise to the fore in the pharmaceutical sector? Consider the following challenges that present opportunities for compliance officers in the industry.

Transparency in Payments

In October 2018 Congress expanded the Physician Payments Sunshine Act to include physician assistants, nurse practitioners, clinical nurse specialists, certified nurse anesthetists, and certified nurse-midwives. Pharmaceutical companies will need to record any monetary payments or other "transfers of value" (conference travel, speaking engagements, consulting assignments, and so forth), and report those payments annually to the Centers for Medicare & Medicaid Services.

Changes in reporting took place again in 2022. The definition of "Covered Recipient" has gone into effect, with five additional provider types now reportable.

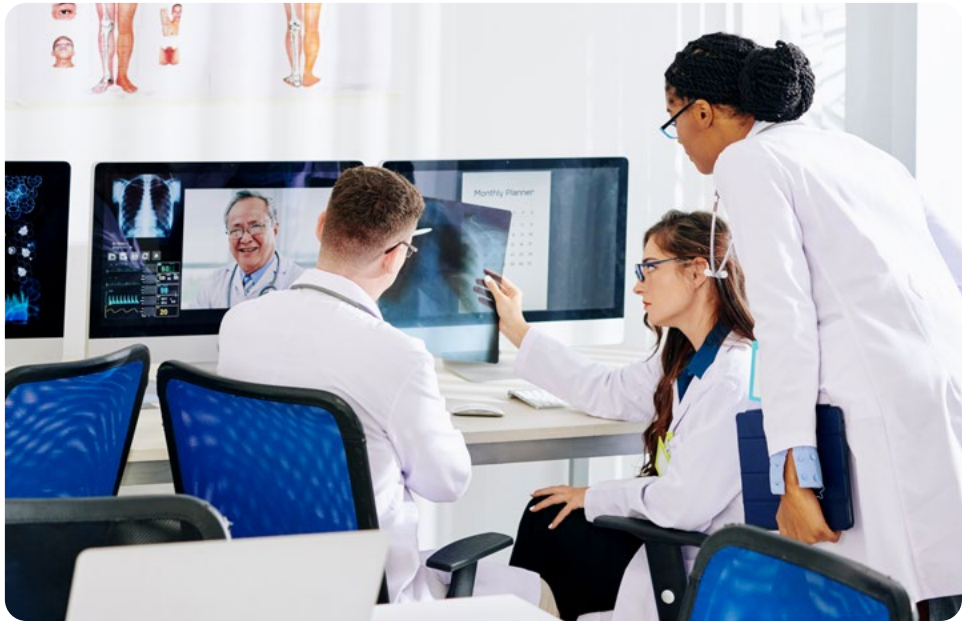
The expanded Sunshine Act reporting will require companies to revisit their policies and procedures for engaging with the newly covered personnel. The compliance department first will need to work with the accounting department to track monetary payments. It will also need to work with the sales department to track other transfers of value, and to assure that those transfers are recorded correctly. That, in turn, may mean new documentation requirements for the sales reps. Training will need to be updated.

M&A and Program Integration

Mergers and acquisitions have long been brisk in the pharmaceutical sector, as larger firms seek to fill holes in their drug development pipelines by acquiring smaller firms, or two large firms consolidate to strengthen their strategic positions. The pharmaceutical world saw 111 mergers and acquisitions in 2018, including 26 deals with valuations projected above $1 billion. Moreover, the value of those deals is likely to rise. Even factoring in 2019's mammoth M&A spending, the top 25 biopharmas by revenue returned nearly US$200 billion more to their shareholders than they spent on M&A during the 2015-2019 time period.

Those trends have several implications for compliance officers. First, they will continue to drive up the importance of performing due diligence on acquisition targets, especially if the target is in an emerging market with higher corruption risk.

Second, after a deal closes, compliance officers will face practical challenges of blending compliance programs: integrating data from various business units, assessing policies that might differ from one unit to the next, deciding how to harmonize policies, training new employees or third parties on compliance procedures, and so forth.



Cybersecurity Concerns

Cybersecurity is a paramount boardroom concern in two ways. First are risks around *privacy*: is the company keeping patient data as protected as possible? A second concern is the risks around *operational security*: is the company protecting its own confidential information as securely as possible? Every year the compliance function becomes more crucial to both matters.

For example, to meet obligations of Europe's General Data Protection Rule (GDPR), the company needs to know which customers are EU citizens (because the rule applies to all EU citizens worldwide); when any customers are conducting transactions in the EU (because the rule applies to all persons within the EU); and whether the company has any personally identifiable information subject to the GDPR.

Those are questions about how the company collects and handles data — which is to say, they are questions about policy and procedure, not IT security.

Likewise, the most common threat to confidential information today is insider threat: an employee or third party sharing data they shouldn't, either deliberately or accidentally. So cybersecurity policy development and training, in close coordination with the IT security and legal departments, will continue to be a top priority for compliance officers.

Patient Assistance Programs

Patient assistance programs (PAPs) have emerged as vehicles for pharmaceutical firms to help the uninsured afford prescription medications. While PAPs can bring many benefits to consumers, they can also pose risks to the pharmaceutical company managing them.

For example, state attorneys general continue to bring enforcement actions against pharmaceutical firms over the opioid crisis or over high drug costs generally. PAPs raise issues of data processing that the compliance function should carefully assess to avoid excessive liability.

Consider the following:

- Should you incorporate patient safety data into the information you collect from patients?
- If you do collect such data, what should the company do with the information, especially if the data suggests a risk of addiction or some other adverse effect?
- If the company outsources the PAP, how can you assure that the correct data is collected and processed in a timely manner?

Compliance functions will need to stand ready with policy management strategies, should senior executives decide to change how a company's PAP works. As with any change in business process, the compliance function will need to assure that policies, procedures, and training stay current with the business's needs.

Foreign Corrupt Practices Act

Pharmaceutical firms always have high risk under the Foreign Corrupt Practices Act (FCPA) because so many of their sales prospects overseas work for government-run healthcare systems, and thus meet the definition of "foreign official" under the FCPA statute.

FCPA enforcement has been brisk for years and shows no sign of stopping in the near future. Compliance officers should, however, consider a few points about FCPA enforcement as they build their compliance programs.

First, the U.S. Justice Department has adopted several policies where it will presume not to impose some of the more expensive consequences of FCPA violations (monetary penalties or independent compliance monitors, for example), if the offending company:

1. Discloses the FCPA misconduct voluntarily
2. Cooperates with any subsequent investigations
3. Remediates any underlying compliance program weaknesses that allowed the infractions to happen

In late 2018, the DOJ Criminal Division Fraud Section's Health Care Fraud Unit announced that it had also started using the FCPA Corporate Enforcement Policy to govern self-disclosures of healthcare fraud and other criminal conduct by healthcare organizations. Compliance functions in the pharmaceutical sector are thus advised to familiarize themselves with the policy.

To reap the benefits of the Justice Department's gentler enforcement for bribery and health-care fraud violations alike, companies must have a compliance program that can meet those criteria. That is, the program must embrace the spirit of good compliance (self-disclosing misconduct) as well as the practical capabilities (investigating and remediating problems).

Second, the Securities and Exchange Commission (SEC) continues its own enforcement of the civil side of the FCPA — and the SEC has imposed monetary penalties, even where the Justice Department has not.

For example, in September 2018 Sanofi agreed to pay $25.2 million in disgorgement, penalties, and interest to the SEC for violating the FCPA's internal control provisions, while the Justice Department had already declined to prosecute any criminal charges. In that case, distributors manipulated weaknesses in Sanofi's accounting policies for discounts and credits to create a bribery slush fund.

The SEC's approach to FCPA enforcement means compliance officers must pay more heed to internal controls, and perhaps even question the wisdom of certain accounting or sales policies. Compliance officers might need to work more closely with the CFO or controller to assess policies, or revisit documentation requirements when someone seeks an exception to internal controls.

CONCLUSION:

Elevate the Compliance Program

Success on all of these issues (and more) ultimately depends on elevating the capabilities and prominence of the compliance program — so that other business functions will want to work with the compliance function, rather than grudgingly allow it onto their turf.

That's a lofty goal and not easy to achieve. Regardless, when one considers all the corporate conduct and regulatory compliance issues facing the pharmaceutical industry, the wisest path forward for pharmaceutical firms is to conduct business in a risk-aware, compliant manner. That can only happen when all parts of the enterprise embrace what the corporate compliance function does and represents.

The truth for pharmaceutical firms is this: enforcement risks will continue; calls for more transparency around pricing will increase; security around data will grow more urgent. The daily operational challenges of running a compliance program will continue to push compliance officers to use technology in new ways, and to work with other parts of the enterprise more often.

Compliance officers need to treat that future as an opportunity. Their objective should be a more empowered compliance program (though the better use of technology), so it can assess and monitor risks with greater insight, and become more embedded (through better training and a stronger culture) so the whole enterprise can navigate the risk landscape with precision and efficiency.

GAN Integrity enables the world's largest brands to do the right thing.

We fulfil our mission by enabling global teams to manage ethics, compliance, and risk with our Integrity Platform, a no-code application building platform.

Seadrill DANONE NORTH AMERICA CLARIOS BARRICK infront

Schedule a meeting to start driving ethical change

To contact us, visit **ganintegrity.com**