POLICY & MEDICINE
COMPLIANCE UPDATE
Reprinted from
Volume 6.7 | July 2020

FEATURE

Monitoring the New Normal

Top 5 Compliance Challenges to Consider in the Changing Digital Workspace

By Manny Tzavlakis, Managing Partner and Louie Karapanogiotides, Manager, Helio Health Group LLC[1]

Summary: While the post-pandemic sales strategy is still out of sight, compliance leaders must act now to ensure their organizations are equipped to handle the systemic changes to monitoring responsibilities caused by the shift to digital field activities. Life science organizations must prepare both their commercial teams as well as their compliance teams to adapt to digital sales interactions in the long-term, equipping them with clear guidance and proper controls in a proactive manner. Amidst the numerous opportunities for change sparked by the COVID-19 crisis, the chance for organizations to rebalance and reorient their Compliance Programs to the digital workspace is one that should not be overlooked.

In the blink of an eye, life sciences companies across all therapeutic specialties had a pressing need to adapt and transform their sales and medical strategies to an all-digital work environment. Before the end of March, global CRM software provider, Veeva Systems, reported sharp spikes in the use of its digital platforms for sales rep-triggered emails and virtual detailing interactions (increases of 400% and 900%, respectively).[2] When Helio Health Group conducted an industry survey a month later, our clients' responses indicated an upswing in all virtual interactions with healthcare professionals ("HCPs") at an approximate increase of 800%.[3] While the shift to digital interactions was meant to be a temporary replacement for traditional in-person field activities, they may become the new normal way of conducting business.

1. Addressing the drastic increase in digital interactions with HCPs.

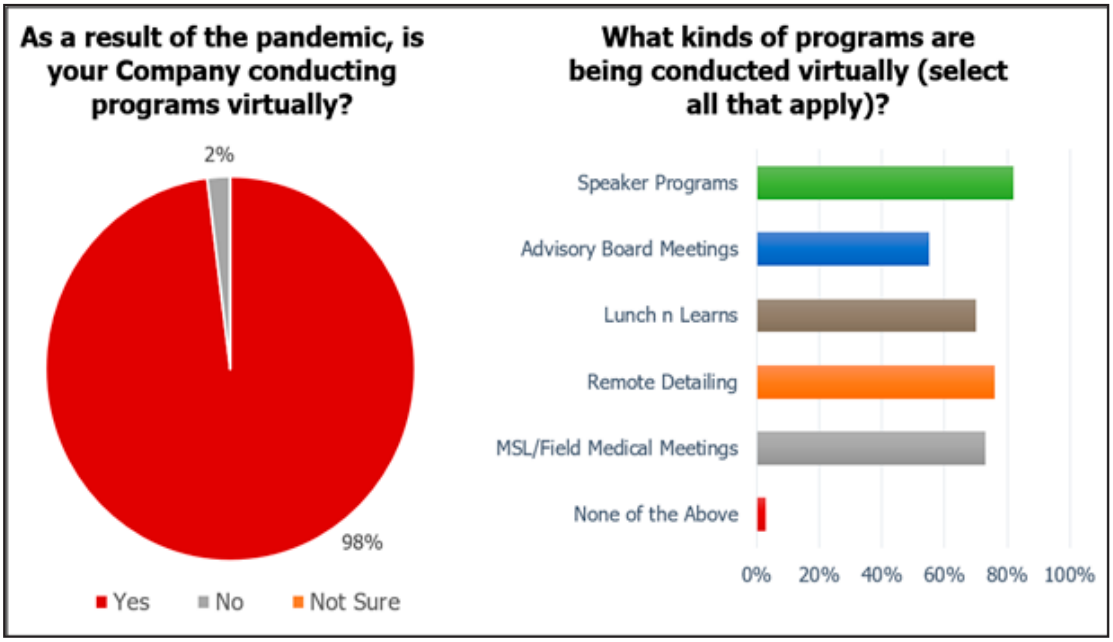
Prior to the onset of COVID-19, life sciences manufacturers invested immense time and resources into developing and improving their commercial and medical strategies, many of which primarily revolved around crucial face-to-face interactions. With this option no longer available, it is no secret that commercial and medical teams have witnessed a disruption in their day-to-day activities. While the post-pandemic sales strategy is still unclear, compliance leaders must act now to ensure their organizations are protected while traditional sales and medical interactions, such as speaker programs, medical field meetings, and office visits, are replaced by web, mobile, or videoconference-based substitutes.[4]

Part IV of Global Health Care LLC's Response to COVID-19 Webinar Series focused on challenges posed by this shift to virtual field activities. The panel surveyed participants to obtain benchmarking of which activities were being conducted virtually, as well as the specific requirements and situations under which they were being conducted.

One aspect, made evident by the audience poll, is that while almost all organizations are conducting at least some virtual programs, companies are divided when it comes to choosing which activities are rolled out

virtually (Figure 1).[5] Companies of all sizes are facing the dilemma of a decrease in face-to-face interactions for the first time; and those companies with solid, tested commercial strategies are finding themselves re-opening and updating old playbooks.

FIGURE 1: *Benchmarking Questions 5 and 6 – GHC Response to COVID-19 Webinar Series Part IV*



Regarding this shift, Cynthia Cetani, Chief Integrity & Compliance Officer at Indivior, communicated to the webinar audience:

> The area we have to think about with [virtual interactions] is, while we might follow the same standards, whether we have the same risks and the same controls. So that's where I think the nuance comes in – where are those controls and where do they need to be?[6]

Regardless of any past compliance program successes, the rapid proliferation of digital programs requires companies to be hypervigilant of the new risks they create. It necessitates that they act quickly to avoid falling behind when it comes to internal controls and compliance-based risk mitigation strategies.

2. Managing business practices that are changing rapidly, but subject to rules and penalties that are largely the same.

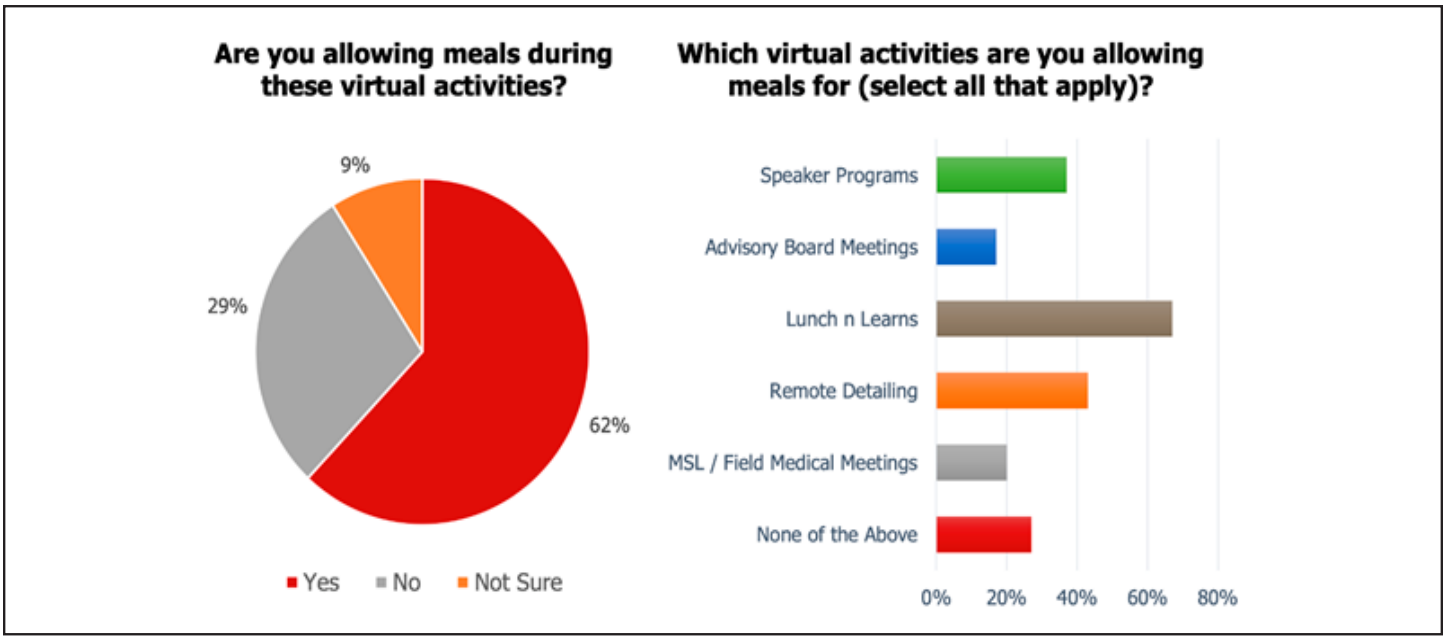
Being pushed abruptly into this new competitive space is unlikely to be viewed by regulators as an excuse for non-compliant behavior. Much of the core legal and ethical framework under which the industry operates, including the Anti-Kickback Statute, the PhRMA Code, and the Physician Payments Sunshine Act, will still apply and be the main lens through which potential regulatory inquiries are viewed.[7]

In the panel's discussion of the evolving logistics surrounding digital programs, Nikki Reeves, Partner and Co-Chair of King & Spalding LLP's Life Sciences and Healthcare Industry Practice, told webinar attendees:

> At the end of the day, the rules are the same. It is still 'business as usual' around who can participate in an advisory board program or a speaker program from the company. And it's still important to make sure that when you have a program that you're conducting, that only those attendees that you know have been invited are actually the ones participating.[8]

The audience poll and resulting discussion highlighted companies' varying approaches towards the ongoing digital transformation (Figure 2). Previous internal controls that governed activities for meals to HCPs, charitable contributions, and Fair Market Value

FIGURE 2: *Benchmarking Questions 7 and 8 – GHC Response to COVID-19 Webinar Series Part IV*



("FMV") rates all had to be re-examined.[9]

While regulators have yet to provide significant guidelines around an all-virtual workspace, it does not indicate that these regulatory bodies are dormant when it comes to making significant updates to policy and guidelines. Life science compliance leaders are still tasked with preparing for industry-specific updates, such as the expansion of The Centers for Medicare and Medicaid Services ("CMS") Open Payment reporting requirements beginning in 2021.[10] They will also be expected to remain vigilant for changes in their organizations' levels of risk in light of continuing updates to the U.S. Department of Justice ("DOJ") Criminal Division's Sentencing Guidelines for the Evaluation of Corporate Compliance Programs (Figure 3).

"While we didn't see seismic shifts with the 2020 Guidance, we did see a number of nuanced revisions,"

FIGURE 3: *U.S. Department of Justice - Criminal Division - Evaluation of Corporate Compliance Programs Updates – June 2020*

Section	Previous Language	Updated Guideline (June 2020)
Section I, Subsection A, Risk Assessments, Updates & Revisions	"Have there been updates to policies and procedures in light of lessons learned?"	"Is the periodic review limited to a 'snapshot' in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures and controls?"
Section II	"Is the corporation's compliance program being implemented effectively? Even a well-designed compliance program may be unsuccessful in practice if implementation is lax or ineffective."	"Is the corporation's compliance program adequately resourced and empowered to function effectively? Even a well-designed compliance program may be unsuccessful in practice if implementation is lax or, under-resourced, or otherwise ineffective."
Section II, Subsection B, Autonomy and Resources, Data Resources & Access	N/A - New guideline added in June 2020 update	"Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?"

said Amy Pawloski, who currently serves as President of Strategic Versatility LLC following her tenure as a lead global compliance executive at Endo International and Bristol Myers Squibb. "These changes collectively highlight DOJ's keen interest in a company's commitment to continually assess risk and strengthen its monitoring program. This includes evaluating operational data and information across functions to monitor compliance risk on a timely basis."[11]

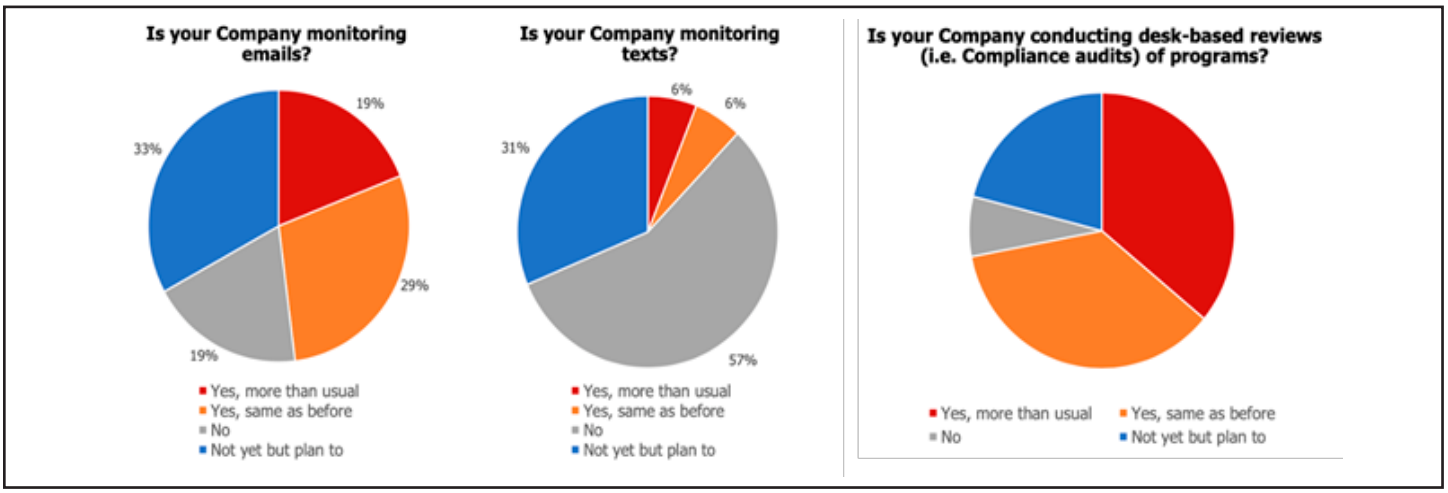
3. Being proactive in adapting monitoring and auditing practices to keep up with the accelerated digital transition.

Perhaps the most pressing action item for compliance leaders will be transitioning their monitoring programs quickly enough to keep up with the explosion in digital interactions with HCPs. On this topic, Pawloski added, "Leading up to the issuance of the 2020 Guidance, DOJ stated in various speeches the importance of a company to analyze its own data for compliance purposes. The formalization of this in the DOJ Guidance simply heightens the expectation that we, as compliance professionals, need to continue to evolve our use of data in ongoing monitoring and analyses."[12] Companies must re-think and re-allocate their resources to maintain oversight of growing digital data sets, particularly emails and texts.

More informal activities do not necessarily equate to less risk when it comes to engaging with HCPs virtually. During discussion of the emerging risks around digital interactions, panelist Stephen Nguyen Duc, Vice-President, Global Head of Human Resources and Ethics & Compliance at Medday Pharmaceuticals, reminded the audience that "there's no difference between a text message and an email in that, as soon as it's written, you can be exposed to something that becomes an issue."[13] The audience polling results showed that companies are moving at different speeds when it comes to monitoring these new risk areas (Figure 4).

As the panel made clear, the uncharted territory of all-virtual commercial activities lifts the importance of executing an effective monitoring program even higher.[14] Ann-Marie Tejcek, Senior Director and Chief Compliance Officer for North America at Eli Lilly and Co., told webinar listeners, "We're not monitoring texts, but there are quite a few investigations around texts...So I think it's really important, whereas maybe we don't have the tools to do the text monitoring, that we take it very seriously and we reinforce our

FIGURE 4: *Benchmarking Questions 19, 20, and 21 – GHC Response to COVID-19 Webinar Series Part IV*



expectations."[15] In addition to areas of increased monitoring, the audience was also polled on which areas their organizations had already established additional guidelines for their employees (Figure 5).

Remote work and the suspension of in-person meetings may cause disruption for compliance teams, especially in desk reviews, risk assessments, and other traditional monitoring procedures. In addition to setting clear rules and guidelines for how to interact with HCPs and patients in a digital space, compliance leaders must consider updating monitoring forms, adjusting FMV tools, and revising risk metrics to ensure their compatibility with a live virtual monitoring program. Just as their cohorts on the commercial and medical side, compliance and risk management executives must continue to re-train their teams, equip them with the appropriate tools, and draw upon the insights available from their organization's internal data in order to better identify and mitigate emerging sources of risk. Monitoring activities will have to be adapted to the new virtual environment but should not be eliminated.

4. Balancing data privacy risks resulting from disruption in medical information.

When it comes to identifying risk, the terms unsecure meetings, unauthorized recordings, and inappropriate distribution of electronic invitations are all new considerations entering the compliance conversation.[16] For advisory boards, speaker programs, and other activities that have shifted to a digital framework, the majority of traditional compliance requirements remain unchanged. However, rolling out "digital sign-in sheets" and other IT-based security solutions have become important discussion points when evaluating the data privacy considerations of digital programs.[17]

While Skype, Slack, Zoom, and other virtual meeting tools serve as a viable replacement for internal meetings, it is important to remember that these programs were not built for use in highly-sensitive, hyper-regulated discussions with groups of external stakeholders. The webinar audience poll pointed to widespread awareness of the still-emerging data privacy concerns

FIGURE 5: *Benchmarking Question 11 – GHC Response to COVID-19 Webinar Series Part IV*

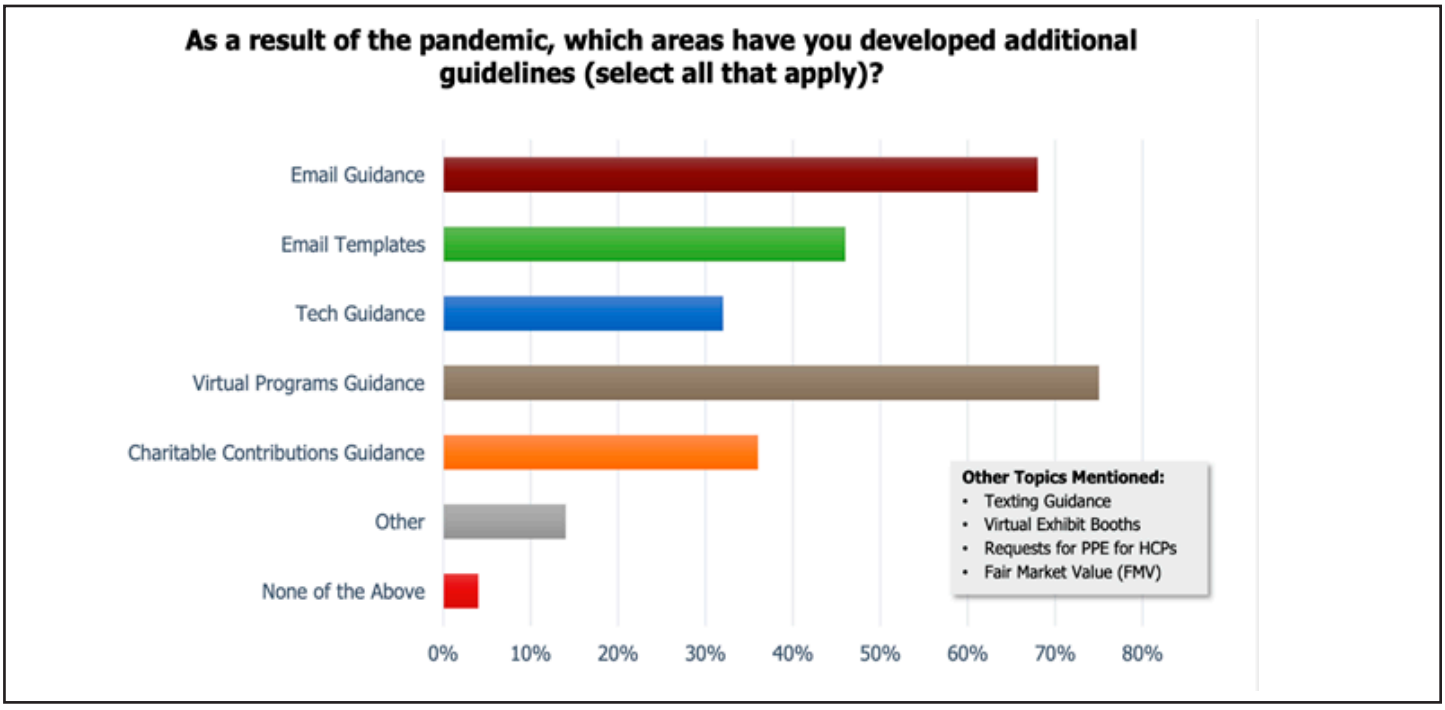
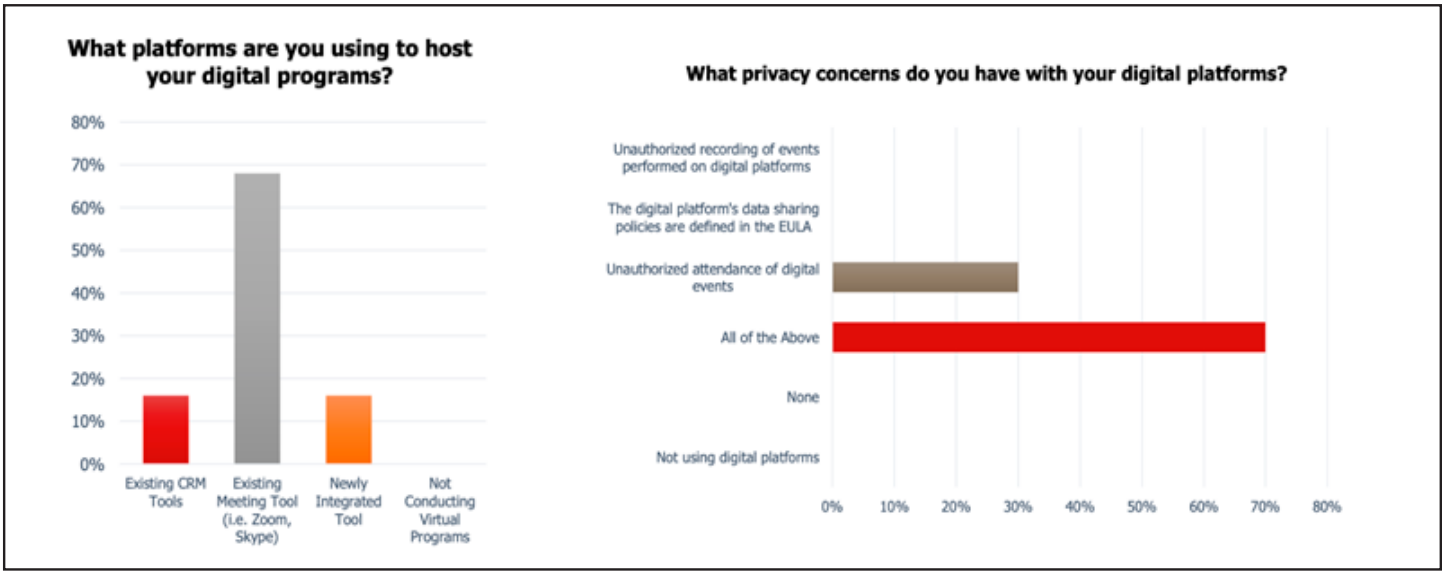


FIGURE 6: *Benchmarking Questions 17 and 18 – GHC Response to COVID-19 Webinar Series Part IV*



associated with increased traffic on digital meeting platforms (Figure 6). Compliance teams should evaluate the technology systems their teams use and ensure that internal controls are put in place to minimize risk.

While organizations have a heightened need to protect the privacy and integrity of their data it comes during a time when Medical Information Request Forms ("MIRFs"), sample requests, and patient services program inquiries are routed through digital platforms at an unprecedented rate due to the limitation of in-office visits and in-person educational programming. The webinar panel encouraged compliance professionals to maintain open, ongoing channels of communication with IT departments as a crucial bridge for reinforcing data privacy controls, while at the same time avoiding further disruption in the flow of medical information to patients and providers.[18]

When we consulted with our own Chief Technology Officer ("CTO") at Helio Health Group, John Poulin, he emphasized that companies should not neglect the data privacy concerns that come from the meta-data generated by digital interactions:

> The DNS and platform-specific tracking traffic created by the expanded use of these platforms is really the most damning from a privacy perspective, and it's also the easiest data to collect. In fact, predatory data aggregators such as Google derive the majority of their profits from tracking and aggregating such data. In the telecommunications world, enforcement authorities often seek the meta-data surrounding phone conversations, which contains information such as who was called, when they were called, and the length of the conversation. The same logic applies to a company's communications made via digital meeting tools (or any interaction on the internet): you may be able to secure the actual contents of a meeting, but the privacy of your company's digital interactions is still at risk if you don't take steps to protect the meta-data.[19]

5. Developing an effective post-pandemic plan: determining what stays and what goes.

There has been no sign that the shift to digital sales interactions will be a temporary one. As companies continue to reevaluate their spending in the current economy, some of these high-cost field activities could be permanently replaced by their temporary solutions.

While the initial months of responding to challenges

posed by the all-virtual environment may have been an exercise in managing exceptions and enacting contingency plans, it's clear that the responsibility of compliance teams does not stop there. Compliance leaders will have an important spot at the table (or the Zoom window) during discussions about what a safe, strategic, and conscientious plan for field activities looks like for their organization whether in-person or digitally.[20]

Conclusion

Compliance programs should be prepared to measure and assess the readiness of their company to handle the temporary and permanent changes to digital activities and interactions. Just as no one can determine precisely when the COVID-19 pandemic will end, no company can be sure how long digital field activities will continue to be a common practice. Organizations must be careful to reinforce Compliance to avoid the compounding risk of "perceived unpreparedness" by regulators, competitors, others in the industry. Amidst the numerous opportunities for change, the chance for organizations to rebalance and reorient their Compliance Programs to the digital workspace is one that should not be overlooked.

References

1 *Helio Health Group is a management consulting and small data engineering-centric firm that specializes in providing consulting services and automated Compliance monitoring solutions across Commercial, Medical, and Patient Services areas of Life Sciences organizations.*
2 *D. Rizzo, Accelerating Digital Engagement in the Wake of COVID-19, Veeva Blog (Apr. 9, 2020), https://www.veeva.com/ap/blog/accelerating-digital-engagement-in-the-wake-of-COVID-19/.*
3 *Id.*
4 *Global Health Care, LLC, Response to COVID-19 Webinar Series – Part IV: Challenges Posed By Field, Commercial & Medical Personnel Change to Digital/ Virtual Promotional Activities in Response to the COVID-19 Pandemic, (Apr. 30, 2020), available at https://pharmaaudioconferences.com/archives/videos/Covid19Part4_20200430.mp4.*
5 *Global Health Care, Webinar - Part IV.*
6 *Id.*
7 *Global Health Care, Webinar - Part IV.*
8 *Id.*
9 *Global Health Care, Webinar - Part IV.*
10 *See CMS, SUPPORT for Patients and Communities Act – Impact on Open Payments, (March 6, 2020), available at https://www.cms.gov/OpenPayments/About/Law-and-Policy.*
11 *Id.*
12 *Id.*
13 *Id.*
14 *Global Health Care, Webinar - Part IV.*
15 *Id.*
16 *Global Health Care, Webinar - Part IV.*
17 *Global Health Care, Webinar - Part IV.*
18 *Id.*
19 *Id.*
20 *Global Health Care, Webinar - Part IV.*

"All risks are not equal."

- Nassim Nicholas Taleb, ***Skin in the Game***

Pharmaceutical, medical device and biotechnology companies continue to receive scrutiny from government entities and the public, leading to increases in investigations, settlements, restrictions and the passing of additional laws and regulations for the industry. As a result, Life Sciences companies are attempting to mitigate these risks by considering new areas of analysis for proactive compliance monitoring.

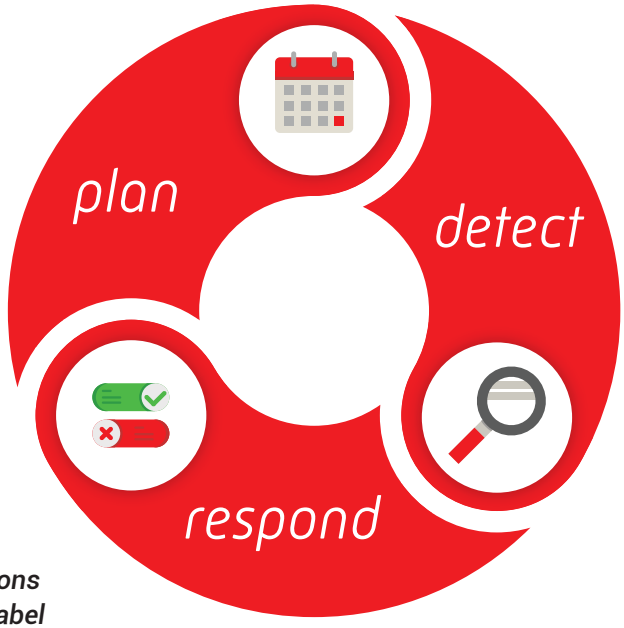
HelioPDR (Plan / Detect / Respond) goes beyond the traditional models of compliance monitoring and utilizes advanced analytics techniques along with our subject-matter expertise to provide a "small-data engineering" approach to risk management in real time. Helio's team of experts have been trained by the Real World Risk Institute (RWRI) specialized course to look for "black swans", unpredictable or unforeseen events typically having extreme consequences.

HelioPDR is a custom human-centered designed, automated monitoring solution that uses integrated data to assist clients with addressing compliance risks efficiently and effectively through: ***Plan. Detect. Respond.***

Plan:
- Develops customizable monitoring plans based on annual business activities.
- Adjusts to respond to changing priorities throughout the year.

Detect:
- Digests numerous data sets (internal & external) to attain insights.
- Assesses and prioritizes compliance risks and adapts approaches.
- Provides simple, customizable workflows to review findings.

Respond:
- Provides simplified workflows to respond to highlighted risks.
- Tracks program performance and risk trends to anticipate and prevent future risk.



HelioPDR is adept at analyzing activities that contain complex sets of data and can provide monitoring with far fewer resources than traditional models. Based on this the following regulated areas are best suited for monitoring via **HelioPDR**:

- ***Anti-Kickback Statute Violations***
- ***HIPAA / Privacy Issues***
- ***False Claims Act Violations***
- ***FDCA Violations / Off-Label***
- ***Transparency / Open Payments***

Key Takeaways

"Small-data engineering" insights

High-design visual dashboard

Proactive monitoring specifications

HELIOpdr

89 Headquarters Plaza North #1443 | Morristown, NJ 07960
201.966.9656 | info@heliohealthgroup.com | www.heliohealthgroup.com

HELIO pdr

a product of Helio Health

www.heliohealthgroup.com/pdr

Manny Tzavlakis
Managing Partner
201.966.9656
mtzavlakis@heliohealthgroup.com