International In-house Counsel Journal
Vol.13, No. 53, Autumn 2020, 1

Managing Compliance Risk in a COVID and Post-COVID World

FABIANA LACERCA-ALLEN
SVP Compliance, Aimmune Therapeutics, USA
LAURA HAMM
Director, Corporate Compliance, Aimmune Therapeutics, USA
BRENDA CRABTREE
Associate Director, Compliance Auditing and Monitoring, Aimmune Therapeutics, USA
TATIYANA AKERS
Corporate Compliance Consultant, Independent Consultant, USA

Abstract: Managing risk can be complicated in the best of times, and the challenges associated with risk management become even greater when combined with the tremendous disruption caused by a global pandemic. In 2020, the world was hit by a global coronavirus disease (COVID-19) pandemic. This pandemic has created many challenges for governments, businesses, and individuals, and created new risk considerations for companies relating to workplace health and safety, privacy, security, employee oversight, and general health and wellness. In managing these new risk considerations associated with the pandemic and ensuring preparedness for future calamitous and yet unforeseen events, companies need to ensure that their own policies and processes relating to crisis management are updated to reflect our new reality. As part of this planning process, companies should consider contingency plans for various potential disasters, both natural and man-made. These plans should include a clear communication strategy, as well as guidance to employees on what actions to take in such situations. With proper planning and preparation, companies will be ready to mitigate the damage that will inevitably come with the next unexpected crisis.

1. Compliance Risk Landscape Before the Pandemic

Risk management has always been challenging, especially in highly regulated industries like pharmaceuticals and finance. Compliance professionals are often tasked with the responsibility of understanding, prioritizing, and mitigating internal and external risks, including:

- Risk stemming from corrupt practices (e.g. bribery, fraud, etc.). This kind of risk may include activities relating to interactions with healthcare professionals, vendors, and other entities outside of the company.
- Workplace health and safety risk, including harm caused to employees or external personnel by accidents or injuries.
- Quality risk, which is the risk that the company will issue a product or service that fails to meet the expected industry standard or violates applicable laws/regulations.
- Environmental risk, which is the risk that damage may be caused to the environment due to company activities or practices.

- Process risk, which is the risk that company processes will fail. This failure may result in violation of applicable laws/regulations as well as failure to meet responsibilities to employees, customers, or the public.
- Social responsibility risk, which is the risk that company business practices may harm employees or the public.
- Compliance risks, which includes risks arising from not complying with applicable laws, regulations, and company policies.
- External risks including data breaches and cyberattacks; natural disasters such as fires, earthquakes, or floods; and attacks on physical security such as rioting and civil unrest.

The global coronavirus disease (COVID-19) pandemic of 2020 has exacerbated many of these pre-existing risks and has also created new risk considerations. The below sections describe several of the new risks that have arisen out of the pandemic and provide advice and guidance on how to manage them in a COVID and post-COVID world.

2. New Risk Landscape and Guidance for Managing Risk

The global pandemic has had the most significant impact on workplace health and safety risk and process risk, due in large part to two primary changes: (1) a large number of employees who previously came into an office setting are now working from home, and (2) for those employees who continue to travel to a workplace, the risk considerations have greatly increased. Working from home brings a host of new challenges including how to ensure proper health and safety, how to manage privacy and security issues, and how to ensure proper employee oversight. Also, all communications are now online for many employees, sometimes creating opportunities for misunderstandings or misuse of the communication equipment. And for employees who continue to come into the workplace, companies must improve and/or develop new processes for ensuring employee health and safety while in the office. In order to overcome these new challenges, organizations need to determine how to manage existing resources and develop plans to prepare for the future. Some questions that leadership should be asking include:

- Which employees' functions are essential and need to be performed at the office, and who can effectively work from home?
- What should our remote/work from home policies look like moving forward?
- Who should ensure that these policies are being followed?
- How can we ensure employees' safety when they return to work?
- What happens if our safety measures fail?
- What are the crisis management procedures and who makes the decisions?
- How are decisions communicated to the rest of the employees?
- Are we prepared to respond to new and unexpected future crises?

The following sections provide guidance for how to manage these new risk considerations, taking into account that there will likely be a "new normal" post-COVID.

2.1 Strengthening Your Corporate Compliance and Ethics Program

At the forefront of risk management and mitigation is the development and strengthening of an effective compliance program. In order to properly deal with the multi-faceted risks posed by COVID and other potentially disruptive disasters, companies must be deliberate and determined in their support to strengthen their compliance and ethics programs. In addition to ensuring adequate headcount and budget, companies must also provide strategic organizational support from all levels of management including the Board of Directors, if applicable. With the appropriate resources and organizational support, an effective

compliance program will enable your company to reduce the risk of potential compliance violations by implementing the following key elements:

- Governance – Designating a Compliance Officer and Compliance Committee
- Implementing Written Policies & Procedures
- Conducting Effective Training and Education
- Developing Effective Lines of Communication
- Responding promptly to detected problems and undertaking corrective action
- Enforcing standards through well publicized disciplinary guidelines
- Conducting Internal monitoring and auditing

Ensuring these elements are established and well-functioning is vital to addressing the ever-changing climate of risk. Compliance teams will need to nurture interdepartmental cohesiveness becuase they will need to work closely with Human Resources, Legal, Information Technology (IT), and Environmental Health and Safety (EH&S) departments to address new risks and regulations resulting from COVID.

2.2 Strengthening Your Environmental Health & Safety Programs

If your organization does not already have a strong EH&S Program, you should consider the budget and staffing requirements needed to help you implement a program aimed at ensuring the health and safety of the environment, your employees, your workplace, and the greater community in which you operate. EH&S Departments will need to conduct thorough research on the new and evolving laws and regulations surrounding COVID and any resulting occupational health and safety measures. This will include a deep dive into federal, state, and local laws in order to stay up-to-date on the most recent guidance.

EH&S Programs include:

2.2.1 Promoting Employee Health and Wellbeing

With more and more companies developing and/or expanding their remote work policies, it is very likely that remote work will become a standard practice in the post-COVID world. We also see a tendency for employees to move to communities closer to their families or with a better quality of life, so now companies will have employees in more diverse jurisdictions and in different parts around the world. Remote work can be very positive, but some employees struggle with social isolation and burnout. To mitigate these potential problems, companies should consider including the following guidance when developing or enhancing their remote work policies to ensure employee health and wellbeing:

- Set clear but flexible expectations for remote work, including expected working hours across time zones and expectations for meetings. This can be especially challenging when, in a crisis like COVID, employees may suddenly find themselves without child or elder care. Setting a positive tone from the C-suite endorsing flexibility, and consistent communication between managers and employees can help reinforce expectations while maintaining flexibility. When working remotely, it may be difficult for employees to separate work and personal time, and this can lead to employee burnout; feeling supported by management can help maintain employee engagement.
- Establish programs and practices that support remote employees. Examples include:
    - periodic regularly-scheduled calls with an employee's manager and team to ensure that employees feel connected and supported;
    - optional informal virtual sessions with company leadership to stay informed on company issues and events;
    - optional virtual "wellness" sessions (e.g. meditation); and
    - optional social events such as virtual holiday picture contents.

- Ensure that remote employees have access to resources and/or equipment that facilitate physical and mental wellness. For example, companies may implement a policy that allows remote employees to obtain ergonomic office equipment.

Companies also need to take measures to ensure employees' health and safety when coming back into the office. Some examples of how to achieve this include:

- Use a health application to screen employees for illness (but note that this has privacy considerations);
- Develop policies and guidance to manage the number of employees in the office at one time, and use a management application that allows employees to schedule time in the office;
- Provide supplies for promoting a safe working environment (e.g. hand sanitizer stations, doors that automatically open, enhanced cleaning protocols, enhanced air purification systems); and
- Establish a clear policy for staying home when sick and ensuring that sick employees are supported, which may require review of the company's sick leave or related policies.

2.2.2 Crisis Management and Enhancing Physical Security

Many offices shut down completely during the pandemic and have remained below capacity to date. This shut-down is a good reminder that in addition to data security, described below, companies should be prepared to provide guidance to employees to help ensure their physical security. During these times of limited staffing, it is important that physical security measures are in place to prevent unwanted visitors from entering facilities. To achieve this, companies should ensure that they have crisis management policies and related processes in place and that these policies and processes are updated to reflect any changes made to company infrastructure as a result of the pandemic, including considerations relating to any updates made to company remote work policies. When developing a crisis management policy, companies should consider the following:

- For the purpose of a company policy, a crisis may be considered any unexpected event that, due to the severity or nature of the event, may place pressure or negatively impact a company's ability to make timely and effective business decisions. A crisis may be internal (i.e. one that directly impacts a company's physical location) or external (i.e. one that affects company employees but does not directly impact a company's physical location, such as a government/agency investigation or an injury caused to a member of the public by a company product).
- The policy should provide the overall framework for identifying and responding to both internal and external crises, which may take the form of either natural disasters (e.g. pandemics, fires, earthquakes, floods, hurricanes, etc.) or emergencies caused by people (e.g. riots, kidnappings, etc.).
- As part of this crisis management planning, companies should develop a communication plan that outlines various escalation chains based upon different scenarios and provides guidance to personnel on "who, what/how much, and when" communications should be disseminated during a crisis. A company may choose to delegate individuals as members of a Crisis Management Committee who are tasked with the responsibility of managing a crisis situation and who would be responsible for executing this communication plan.

2.2.3 Emergency Action Plans

As a supplement to a crisis management policy, companies should also develop and/or update their Emergency Action Plans to reflect any changes caused by the pandemic (e.g. changes to office locations, changes in the number of personnel working remotely, etc.). Emergency Action Plans are comprehensive guidance documents developed by the company's EH&S and/or Safety Committee members for company personnel to reference when preparing, preventing, and responding to workplace emergencies at Company offices. These documents consolidate emergency response and prevention procedures, including both general and incident-specific procedures, for company personnel to follow during workplace emergencies in order to minimize injury, harm, hazard, and/or property damage. Companies should have an Emergency Action Plan for each physical site location, and these plans should include site-specific information covering the following topics, as applicable:

- Company emergency notification and reporting systems
- Company chain of command and emergency contact list
- Emergency evacuation procedures and emergency escape routes
- Shelter-in-place procedures
- Guidance for company personnel performing rescue and medical duties (e.g. the company may ask for volunteers to be a part of the company's volunteer emergency response team)
- Injury and illness reporting
- Fire safety and prevention plan
- Responding to potential local natural disasters (e.g. earthquakes, flooding, severe weather, etc.)
- Workplace violence
- Active shooter
- Trespassers/criminal activity
- Civil disturbances
- Terrorism/hostage situation
- Bomb threats/suspicious items
- Biological hazards
- Chemical/hazardous materials spill and release response
- Power outages
- Remote access of company office phone lines

All employees at each site should be trained and receive periodic review of the site's Emergency Action Plan. Additionally, companies may conduct live simulations/trainings of various crises so that employees are able to practice some of the responses (e.g. building evacuation procedures) to be better prepared in the event that a real emergency situation arises.

2.3 Enhancing Data Privacy and Security

In addition to the challenges posed to health and well-being stemming from the pandemic, it may also be more difficult to manage data privacy and security considerations when many more employees are working outside of the office. To start, companies need to evaluate new in-house versus remote needs with regards to IT hardware, systems, and infrastructure and make additions and/or enhancements as needed to support the remote workforce. In addition to these evaluations, companies should update their data privacy and security policies as needed to reflect any changes in systems and infrastructure to

enhance the security of remote work situations. When developing these policies and processes, companies should take into consideration the following:

- Some employees may not have a dedicated, private workspace outside of the office. Guidance (e.g. best practices for working remotely) and resources (e.g. privacy shields, headsets, etc.) should be provided to employees as needed.
- Employees may not be used to the handling and storage of sensitive, confidential, and/or proprietary information outside of the office, and guidance should be given on how to handle this information in a secure manner, including practical suggestions for communicating or maintaining sensitive information in a workspace shared with family members or roommates.
- Companies should have a process for responding to data breaches, and this process should be publicized to ensure that employees know how to respond in the event that data is either received or released in a manner that violates company policy and/or applicable law (e.g. General Data Protection Regulation).
- Employees should be trained to be sure that they understand the updates made to any policies and processes.

2.4 Ensuring Oversight of Company Activities

As discussed above, with more and more people working remotely, companies will face the challenge of ensuring proper employee oversight. To provide effective oversight, companies first need to set clear expectations, as outlined above. Employees must be trained on these expectations, and trainings should be updated as needed to ensure that employees understand the expectations. Companies must also ensure that employees have the proper resources to meet these expectations.

Once expectations are set, and employees have been given the proper training and guidance to meet them, companies can conduct enhanced monitoring (e.g. expense monitoring) and review to ensure that employees are meeting expectations. Managers should be involved in this review process and should help conduct any supplemental training to ensure that the company is conducting proper oversight while supporting remote employees to ensure that everyone has the opportunity to succeed.

2.5 Business Continuity Planning - Preparing for Future Crises

Business Continuity Planning involves developing a comprehensive plan of action in the event of an unforeseen disaster to help minimize downtime/disruptions and restore business operations. This is one of the best tools companies can use to prepare for the future disasters in an efficient and cost-effective manner. Business Continuity Plans (BCPs) complement Crisis Management and Emergency Action Plans, described above, in that BCPs provide additional guidance for companies in the event that a crisis leads to long-term disruption of regular business operations rather than a short-term emergency situation.

Business Continuity Planning involves:

- Conducting a Risk Evaluation and Business Impact Analysis – Business functions are classified as critical, important, or non-essential; operational & financial impact resulting from the disruption/loss of the individual business function/process is determined, recovery times are defined, and recovery resources are identified
- Identifying roles and responsibilities for business continuity recovery teams
- Identifying each department's disaster identification, response, and recovery team decision-making processes and communication plan
- Developing Disaster Response and Recovery Plans including identification of categories (e.g. labor via employees or third-party vendors, physical sites, equipment, technology, etc.) and quantity of resources required to implement disaster response and recovery procedures

- Developing specific Business Function/Process Recovery Procedures - These plans/procedures should include establishing:
    - working groups and workflows for restoring critical and important business functions/processes
    - the timeframe for restoring critical and important business functions/processes
    - actual steps/procedures required to respond and restore critical and important business functions
    - alternate site operations
    - contact and utilization of internal and external resources
    - online access and manual workarounds to company and department-specific systems if needed
    - communication plans
- Identifying current document retention and back-up processes for vital records, hardcopy files, forms and supplies if needed

Training, testing, and maintenance exercises will also be vital to ensuring a well-functioning business continuity plan is in effect and operational.

Companies should always be prepared for the unexpected. As we have witnessed in 2020, crises manifest abruptly and affect people and business in unforeseen ways. But companies can be ready to respond to these situations by having the right plans, policies, and procedures in place; by training their people on these plans, policies, and procedures; and by conducting periodic review to assess any changes to the risk environment and make sure that all documentation and training is up-to-date and reflective of the current environment. Additionally, it is important to surround yourself with people of integrity who you trust and who you know will act responsibly in a crisis situation. And open, transparent, and timely communication is key.

***

M. Fabiana Lacerca-Allen has over 30 years of experience in legal and compliance roles, working for leading American companies such as Aimmune, Elan, Mylan, Bristol-Myers Squibb Company, Microsoft, Merck, and AT&T. She has counseled and litigated in the field of international business transactions and international environmental law. She has extensive experience in the pharmaceutical industry in leadership roles in charge of legal and compliance teams. She has counseled and represented clients on a broad range of questions, including strategic business initiatives ensuring compliance with laws and regulations, and corporate policy. Ms. Lacerca-Allen has provided legal support and strategic advice on opportunities and trends in law particularly within the government sector, as well as with major and strategic corporate accounts. Fabiana has established policies and oversight on key areas of compliance affecting international markets, and she has been able to positively impact the perception of compliance, creating compliance training programs and relevant standard operating procedures and has been involved in validating and aiding due diligence in the compliance industry, frequently being requested as speaker and participant in forums. She has been recognized in the industry by Hispanic Executive Magazine in 2013, http://hispanicexecutive.com/2013/fabiana-lacerca-allen/; recognized as 2015 Women in Leadership, Inspiring Leaders: http://www.theguardian.com/women-in-leadership/2015/may/12/know-who-you-want-to be-kidnapped-with-and-four-more-tips-for-leaders; served as Chair to the Bay Area Ethics & Compliance Association (BECA); and served as Co Chair for CBI, an Advanstar company serving the Life Sciences industry. Ms. Lacerca-Allen was invited to join the Gioja Research Institute while she was a student researching on environmental law. She was recipient of 1992 UCLA's tuition waiver based on merit and recognition, and she

represented UCLA in the Roscoe Foundation National Essay Contest submitting a paper on Global Warming.

Laura Hamm is the Compliance Director at Aimmune Therapeutics. Before joining Aimmune, Laura was the Compliance Officer of medical device manufacturer Stryker's Neurovascular division, a nearly $1B business, and Stryker's only global division. At Stryker, Laura oversaw all elements of Neurovascular's compliance program. As a global Compliance Officer, Laura has witnessed the evolution of international regulations, and recognizes the importance of cross-border collaboration to meet global business goals. Laura is passionate about integrating compliance into business DNA, and empowering business partners to achieve objectives with high integrity. Prior to industry, Laura was an educator in the California public school system, focusing on literacy in low-income communities.

Brenda Crabtree is the Associate Director, Compliance Auditing and Monitoring at Aimmune Therapeutics. Prior to this, Brenda worked as an intellectual property attorney for biotechnology and pharmaceutical companies and advised pharmaceutical and medical device companies on various compliance matters including corporate policy and strategy, privacy, transparency, and fair market value. Brenda is a humanitarian who began her career in public service as a U.S. Naval Officer, and she applies her strong sense of "doing the right thing" to her work as a compliance professional.

Tatiyana Akers is a Corporate Compliance Consultant with over 12 years of Legal, Financial Services, and Compliance experience, specializing in the development and implementation of global ethics and compliance programs within the Pharmaceutical Industry. She has assisted pharmaceutical companies with the successful implementation and management of Office of Inspector General (OIG) mandated Corporate Integrity Agreement (CIA) obligations, including the development of CIA specific training; policy development; annual Independent Review Organization's (IRO) system and transaction reviews; management and accountability certifications; board of directors resolutions; disciplinary guidelines; conflicts of interest, exclusion screening, and disclosure programs; as well as implementation/annual reports to the OIG. Mrs. Akers is also an experienced compliance investigator, partnering with various business functions to respond to, identify, and remedy potential compliance violations. She has a strong desire to integrate compliance initiatives and ethical practices cross functionally and via corporate leadership to ensure optimal compliance and operational efficiencies within organizations.

Tatiyana Akers works as an independent consultant to pharmaceutical companies in the San Francisco Bay Area assisting with the implementation of comprehensive compliance and ethics programs

Aimmune was created in response to a united call to action from the leading minds and key stakeholders in food allergy who met at an advocacy-sponsored research retreat in 2011 to reach consensus on the direction of food allergy treatment research. Among the outcomes of the retreat, the group concluded that a standard oral immunotherapy (OIT) approach needed to be established, and associated products needed to be developed. When no pharmaceutical company showed interest in developing an OIT treatment, the food allergy community formed Aimmune. Today, Aimmune is working to fulfill the 2011 shared vision of developing a peanut allergy treatment and making it available to allergists for patients worldwide.