ASHVINSGROUP
TECHNOLOGY PROFESSIONALS

7205 Corporate Center Dr, # 504
Miami, FL 33126
305-264-4442
www.ashvinsgroup.com

IT QUALITY & COMPLIANCE IN FDA REGULATED ENVIRONMENT

Client Profile:

A leading pharmaceutical company that develops and delivers medicines and vaccines.

Technologies Used:

Evidence collection (collecting data needed to effectively manage IT security), frameworks to automate compliance (SOC2, HIPAA, PCI, GDPR), security policies, analytics and Shift Left Approach (focus on risk management and prevention). Technology alone is not enough, there needs to be a culture of compliance with strong governance and collaboration across functional groups.

Project Summary:

Client was transitioning to new Application Lifecycle Management (ALM) and Complaint Management (CMS) computer systems. The End-of-Life phase is the final stage of the systems life cycle. This included decommissioning, retirement and archiving the system. Once data is migrated, hardware can be released and repurposed if required. Once the system has met its retention period and there are no other holds on the system, the data is purged. Upon initiation of a system and throughout the lifecycle, it was important to identify all components (hardware, software, documentation, database). This was critical in order to ensure that the End-of-Life cycle retires the entire system. The procedure applied to all IT delivered solutions (system service, application, platform and mobile application regardless of size or complexity. Understanding the client's compliance technology maturity is also important. Too little effort and you compromise product quality. Too much effort and you can overwhelm the IT teams. We developed a strategic, balanced and sustainable approach to End-of-Life and transitioning compliance. A comprehensive compliance implementation helps to prevent FDA Form 483 observations, warning letters, recalls and regulatory meetings. All aspects of the End-of-Life Phase must be documented including SOP that identifies each of the deliverables required for each system (GxP and Non-GxP).

Compliance risk areas evaluated in this project included cybersecurity, governance practices, privacy and managing conflicts of interest within the organization. Compliance risk management involved proactive planning, continuous monitoring and leadership.