HCLTech | Supercharging Progress™

Cloud migration in pharmacovigilance

In the pharmaceutical industry, pharmacovigilance (PV) plays a vital role to ensure the safety profile of a drug and strengthen patient care at large. The PV departments are under enormous pressure to transform into proactive and intelligent functions while reducing costs and remaining compliant with continually changing regulations worldwide.

PV departments are facing numerous challenges such as increasing case volumes, regulatory compliance, limited budget and resources, industry complexity and the need to process new signal detection data. They are also burdened with legacy on-premises applications that lead to increased costs and challenges around accessibility, user experience, performance, data security and compatibility.

To tackle these issues and overcome them, cloud technology provides highly scalable, cost-effective, data-secure and privacy-compliant solutions. According to Gartner research, more than 70% of companies have now migrated at least some workloads into the public cloud.

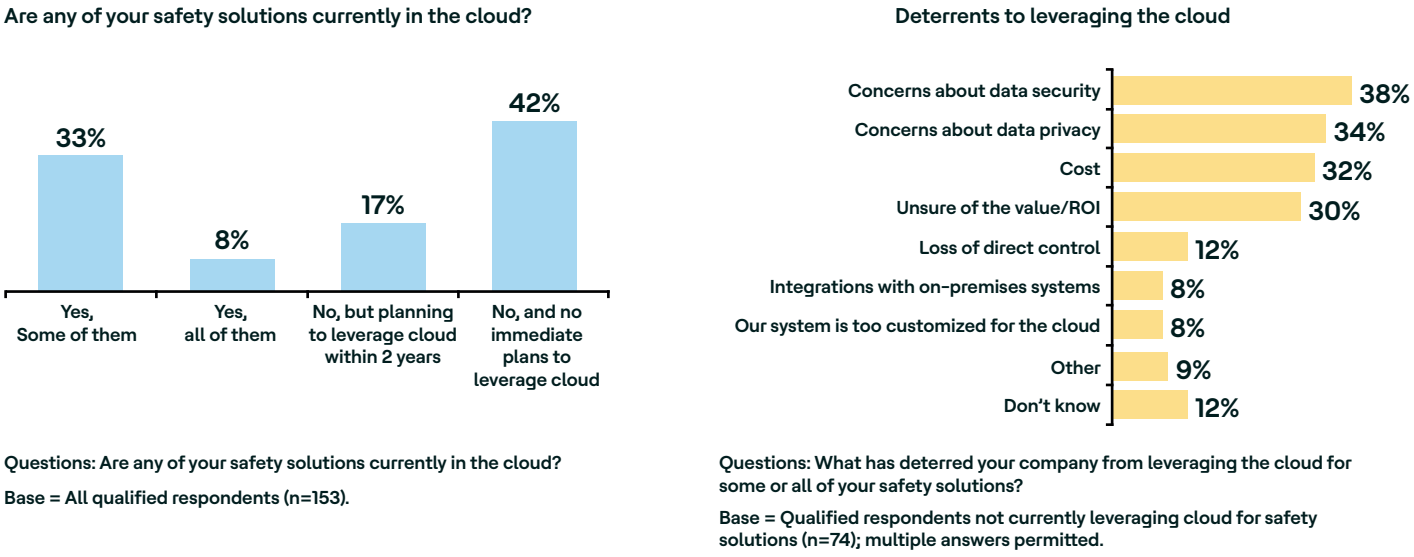


Fig 1: Barriers to leveraging cloud technology

Service models

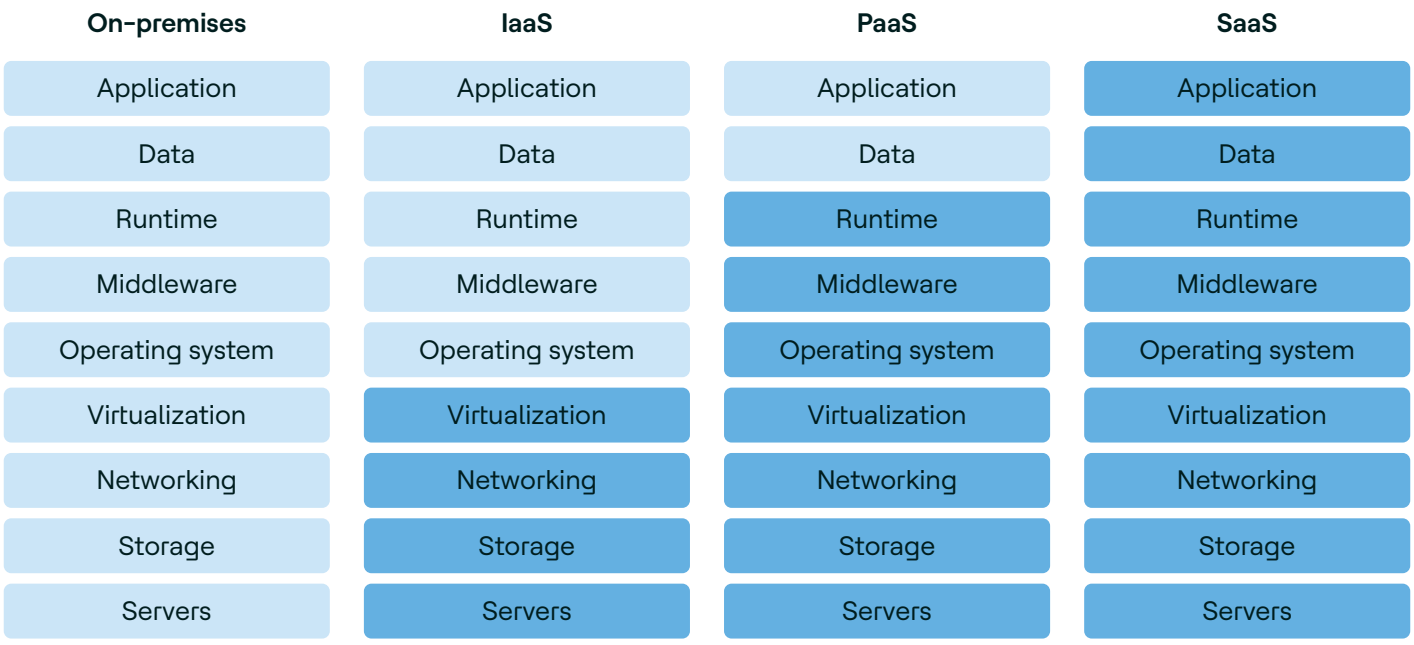


Fig 2: Different service models and shared responsibilities

The service models for pharmacovigilance operations, including on-premises, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), are not mutually exclusive. Mid-sized pharma organizations, which include PV functions, often utilize multiple service models. Similarly, large organizations commonly employ a combination of all service models depending on their specific business needs. The deployment method can vary too, with organizations opting for either public cloud or hybrid cloud deployment.

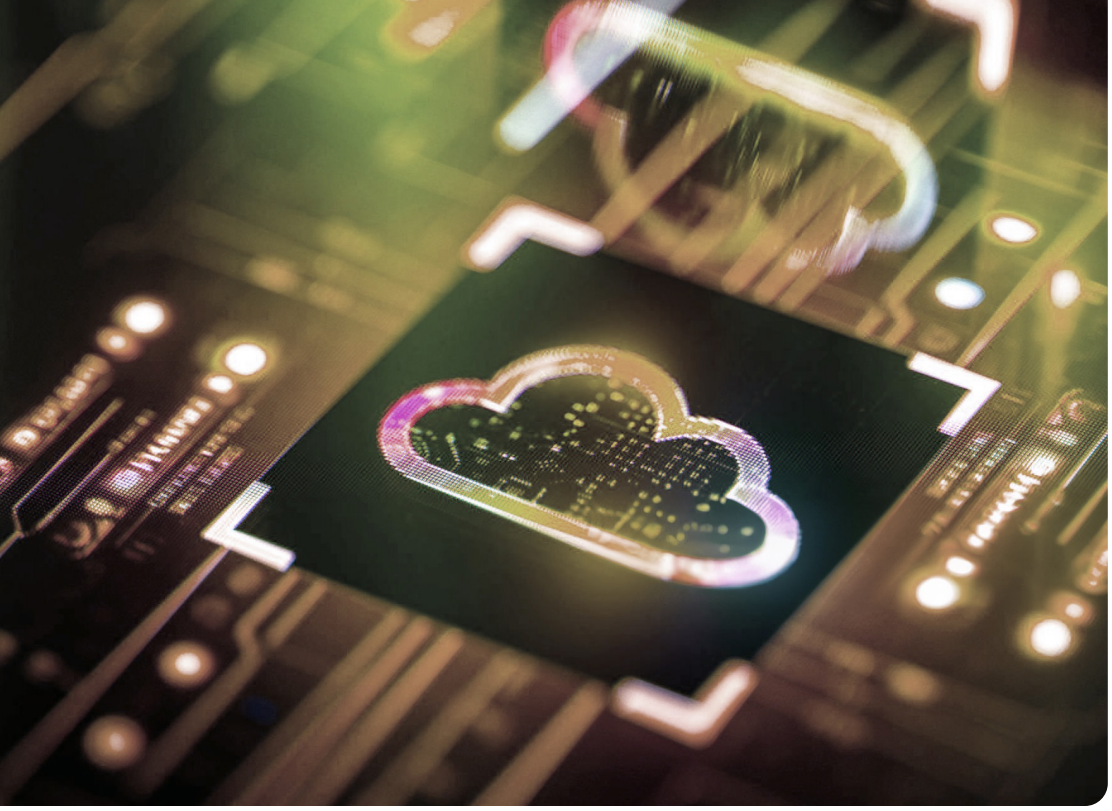
Deployment models

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization, a third party or in collaboration, and it may exist on or off-premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off-premises.

Public cloud: The cloud infrastructure is provisioned for open use by the public. It may be owned, managed and operated by a business, academic institution, government organization or a combination of them, and exists on the cloud provider's premises.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).



Cloud adoption – Key considerations

In our experience, when defining a cloud transformation strategy, it is essential to consider the following key factors for making appropriate decisions on selecting the service model (on-premises, IaaS, PaaS and SaaS) based on specific business needs.

Enterprise IT strategy

While defining the IT strategy, the PV department should align with the organization's digital transformation strategy. A few years back, pharma organizations were reluctant to adopt cloud migration technology considering the amount of sensitive, intellectual and regulatory data they are responsible for. After a long period of resistance, pharma organizations are increasingly harnessing the power of cloud computing to reduce costs and streamline their workloads. Pharma organizations are fully embracing their move to the cloud to streamline the process of clinical research, drug discovery and development. Cloud technology can help pharma organizations enhance their process efficiency, speed and facilitate discoveries to meet the unmet needs of patients.

Hence this is the right time for PV departments to reassess and align their strategy with the enterprise's strategy.

Case (adverse events) volume

Irrespective of the size of a pharmaceutical organization's drug portfolio, or the volume of adverse event (AE) data processed by the pharmacovigilance department, cloud technology presents an opportunity to elevate efficiency, accelerate processes and optimize costs. PV departments have now embraced the potential of cloud storage, enabling them to handle vast amounts of data with ease.

For smaller organizations, it is important to consider if SaaS-based solutions offer a more cost-efficient alternative. SaaS operates on a pay-as-you-go model, where costs are directly tied to the data processed, eliminating the need for traditional licensing approaches. This innovative approach presents captivating advantages in terms of flexibility and costing.

However, it is possible that these solutions may not wholly align with the unique business requirements of the PV department, ultimately resulting in limited customizations and control.

Shared responsibility

It is critical to understand the shared responsibility model to ascertain which security tasks are handled by the cloud provider and the PV department respectively. Responsibility and ownership of how applications are managed in the cloud vary depending on the service model - SaaS, PaaS, IaaS or in an on-premises data center.

In every cloud deployment, the ownership and security of data and identities lie firmly within the realm of the PV department. Whether undertaken by the PV department itself or entrusted to the broader pharma organization, the PV department assumes full responsibility for safeguarding these vital assets

- Data
- Endpoints
- Account
- Access management

By adopting cloud technology, the PV department can shift day-to-day security responsibilities to cloud providers and effectively leverage cloud-based security capabilities to improve threat detection and response time. By shifting responsibilities to the cloud provider, organizations can get enhanced security coverage, enabling them to reallocate security resources and budgets to other key business priorities.

Future growth

In this age of social media, chat groups, registries and the demand to process real-time signals, the volume of adverse event data received by pharma has tripled. In addition, companies are proactively monitoring and tracking new "secondary use" data sources such as electronic healthcare records, administrative claims data, social media, web search logs and pharmacokinetics and genomics data for potential signals, increasing AE data to be processed.

As per the US FDA Adverse Event Reporting System (FAERS), the number of AEs reported has increased from 933,232 to 16.814 million in the last decade. The infrastructure must consider the growth in the volume of data and the cost associated with infrastructure procurement and maintenance (demand with scalability and cost associated to procure and maintain the infrastructure).

Cloud data center location

Generally, the pharmacovigilance function or staff is located globally where country organizations or clusters are responsible for processing local AE reports and route the information through the central PV department for further processing and expediting. The central PV department is located at one or two sites to support businesses exception, except where the central PV department of large pharma organizations operates from multiple global locations to manage case volumes. The location of the cloud data center is arguably a key consideration for better performance and benefits from low latency and multiple redundant bandwidths. On the flip side, poor location can result in unstable connections and efficiency problems.

Cloud provides the flexibility of deploying the resources in desired global locations, where the public cloud provider already has an infrastructure, and an organization can just lease the services with a pay-as-you-go model. This also gives flexibility to pharma or PV departments with a vision to expand their global footprint.

Customers can also benefit from edge locations, which are cloud data centers designed to deliver services with the lowest latency possible. Cloud service providers have dozens of these data centers spread across the world. Country organizations can have similar experiences in accessing and using safety systems as central sites.

Capital Expenditures (Capex) and Operating Expenses (Opex)

A shift from Capex to Opex is one of the key factors influencing the PV department in adopting cloud technology. It has become a well-known fact that organizations can optimize costs on hardware and data centers by buying services on an as-needed basis. This also reduces the maintenance and upkeep overheads for the PV department.

By adopting the pay-as-you-go model, businesses can reduce the risk of a large upfront capital investment and access a predictable, monthly payment structure. This shift towards an operational expense approach can enable companies to remain agile in the ever-evolving manufacturing industry.

For example, an analysis from Everest Group has highlighted the significant increase in pharmacovigilance spending. Over the last decade, annual spending reached more than triple the percentage of sales - from 0.3% in 2003 to over 1% in 2017.

Challenges to cloud adoption

As PV clients transition from an on-premises data infrastructure to cloud technology, they may encounter several key challenges.

Data privacy

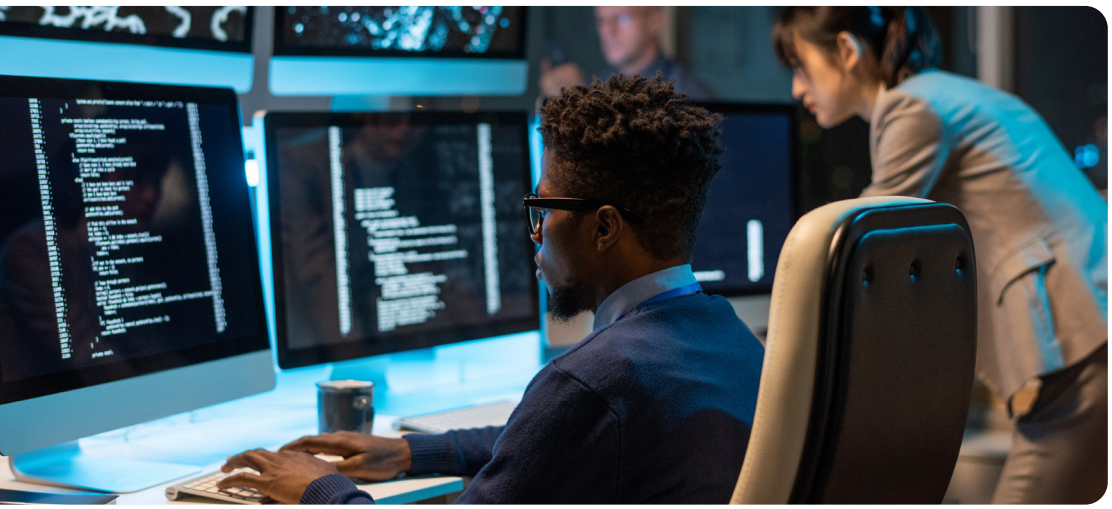
Pharmacovigilance is a function that deals with the sensitive and personal data of patients. Many emerging laws, particularly those dealing with privacy and personal data, require that the data is secured, and businesses comply and report on compliance and any breaches that occur.

Opting for cloud technology involves the storage of data at an off-site location, making the physical location and security of off-site data centers important.

Below are mandatory requirements from the PII (Personal Identifying Information) which should be considered when processing personal data in the cloud.

- Data subject notification
- Right to use and disclose
- Data collection
- Data usage
- Data sharing or transfer
- Data disposal or retention

Security policies must be at the forefront of any cloud or on-premises solution. It is no longer sufficient to solely understand existing laws and regulations such as GDPR, HIPAA and PCCI that govern the collection and storage of personal data. As global data privacy rules continue to evolve (like the recent implementation of the China Personal Information Protection Law (PIPL) on November 1, 2021), PV security experts must proactively evaluate and ensure that the latest rules and regulations are implemented to ensure compliance with data regulatory mandates.



Security

As pharmacovigilance is a highly regulated function, security has been the number one barrier to cloud adoption. In the last decade, cloud governance and security features have evolved to address the needs of highly regulated sectors.

Data in the cloud can be in one of four phases: data in motion, data in use, data at rest and data in stasis. It is important to protect PV data in all four phases by implementing preventive and detective security services.

Infrastructure sizing for hybrid cloud computing

To make informed decisions on what to migrate to the cloud and what to keep on-premises, cloud architect teams must comprehensively analyze the current environment. This entails studying various factors, including physical equipment and data center lease timelines, license validity, the possibility of transferring licenses to the cloud resources, compatibility of applications, services and platforms and availability of cloud support.

Preparation begins with an assessment of the existing infrastructure and a migration plan. The exact capacity of physical or virtual infrastructure resources should be calculated based on current volumes and the capacity for future growth.

Data migration

Any data migration strategy includes the 6Rs: Rehosting, Re-platforming, Repurchasing, Re-architecting, Retiring and Retaining. For any PV data migration, it is important to ensure there is minimal downtime to minimize the impact on regulatory submissions and productivity. Another important factor to ensure is that there is no loss of AE or submission data and that all PV data transformation logic is well-validated and traceable. Hence, before initiating any cloud migration, it is critical to understand the available strategies and tools to accelerate PV data migration and help meet project goals and timelines.

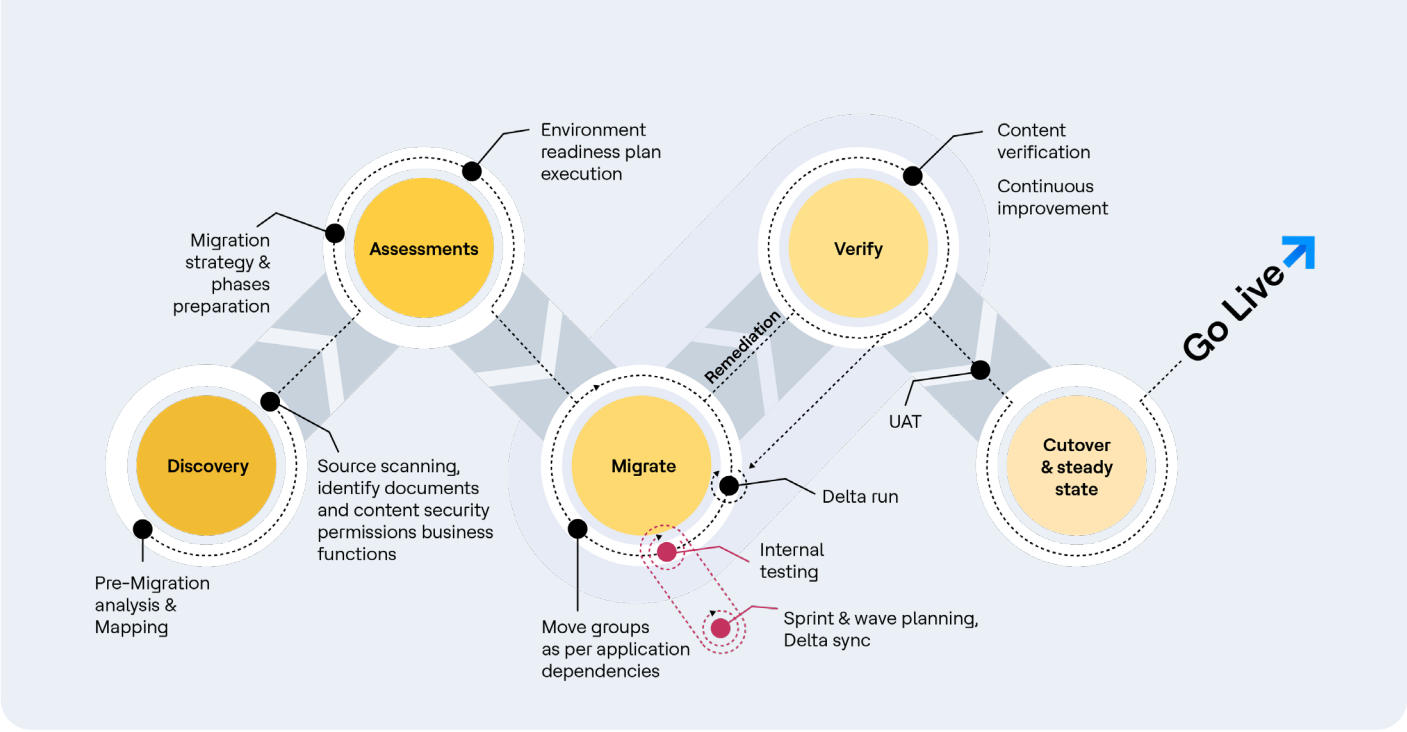
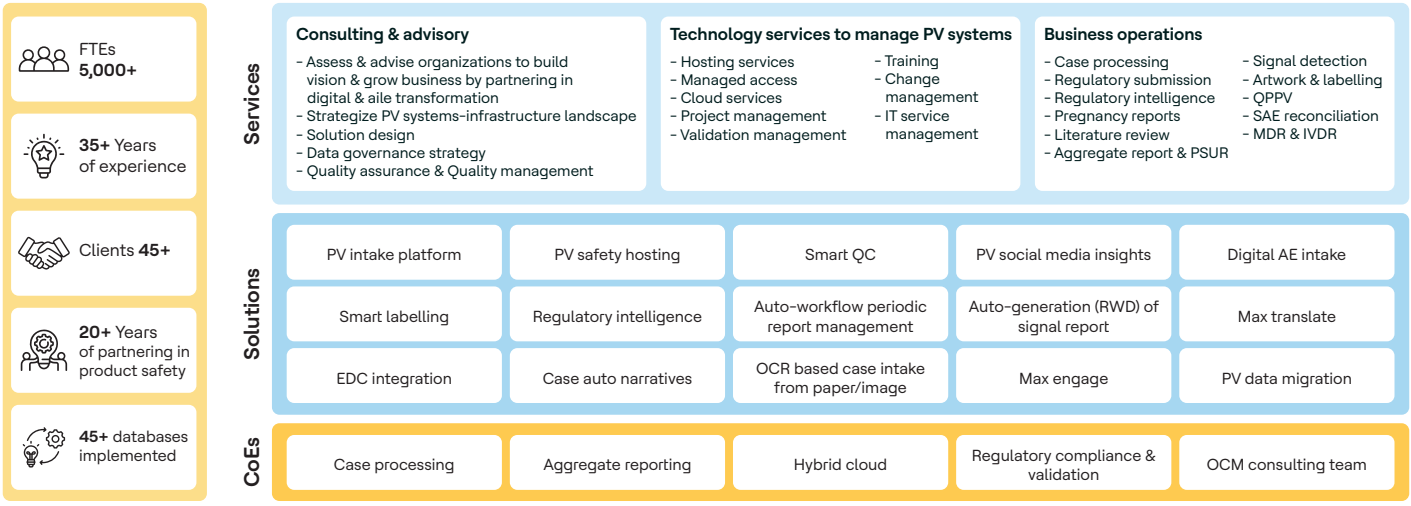


Fig 3: Migration cycle overview

How can HCLTech support cloud migration in PV?

The main drivers for cloud-based movement are to optimize applications and infrastructure and reduce cost. Based on the enterprise's digital and IT strategy and current PV business needs, PV departments can choose to either continue with the traditional approach (on-prem) or move to new technology platforms leveraging hybrid cloud computing (through Azure, AWS, Google or Oracle cloud platforms) or SaaS solutions (Oracle, Veeva, IQVIA).



HCLTech can help evaluate the current PV system landscape and advise on future PV digital strategy considering the factors detailed above. Our team has vast experience, technical knowledge and domain expertise to drive cloud implementation for PV clients. HCLTech's PV and CloudSMART CoE help PV clients decide on a cloud adoption journey aligned to their business strategy and objectives. Agility, resilience and scalability are the factors considered while designing an outcome-based, robust digital transformation strategy.

We leverage our extensive experience and innovative approach to guide you with industry best practices, data privacy and governing regulations, PII, associated risks and effective mitigation plans.

Author

Kiran Singh J
Associate General Manager, HCLTech

Kiran is a seasoned Practice Manager with over 14 years of expertise in Pharmacovigilance and medical information within the pharmaceutical industry. He has a proven track record of leading successful digital transformations in Pharmacovigilance, Medical Information, Regulatory, Aggregate Reporting and Medical Writing. Kiran excels in delivering innovative solutions and enhancing operational efficiency across these domains.

co-author

Vishal Mandlik
Group Manager, HCLTech

Vishal Mandlik is a seasoned pre-sales Solution Architect with over 14 years of experience in Hybrid cloud Infrastructure services. He has expertise in on-premises, private and public cloud hosting, migration and support dedicated to life sciences and healthcare client portfolios. He designed the solution for multiple migrations of on-premises and cloud workloads and modernization of infrastructure to PaaS platform for healthcare customers, leading to cost and effort optimization through a shift from a Capex to Opex model and thus also helping customers leverage the benefits of different modern cloud services through a cloud native backbone followed by steady-state support structure for hybrid cloud IaaS and PaaS platforms.

HCLTech | Supercharging Progress™

HCLTech is a global technology company, home to more than 227,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending March 2024 totaled $13.3 billion. To learn how we can supercharge progress for you, visit hcltech.com.

hcltech.com