Ensuring GMP Compliance with Lab IT Infrastructure and Systems

Continuous improvement is an essential priority for pharmaceutical manufacturers. This push for continuous improvement is one of the reasons companies invest in their IT, including lab IT infrastructure and systems. As a result, more and more processes and workflows in pharmaceutical laboratories are being completed on computerised systems, making GMP compliance an increasingly important consideration.

New technologies, particularly those that automate or semi-automate processes and workflows, make pharmaceutical manufacturers more competitive. A modern IT infrastructure, advanced computerised systems, accelerated use of virtualisation technologies, and cloud computing also reduce costs while increasing operational process efficiency, performance, management, protection, and the efficient use of resources.

New technologies also help pharma companies adhere to regulations and improve product quality and safety.

GMP – Good Manufacturing Practice – is a quality assurance system designed to maintain the quality of manufactured products, as well as ensuring they are safe and effective. GMP applies to all parts of the manufacturing process, including those elements that take place in the lab. Therefore, it is essential to ensure GMP compliance with your lab's IT infrastructure and systems.

GMP vs GLP

GLP – Good Laboratory Practice – is also a quality assurance system but it is different from GMP.

In general, GLP covers the research and study phases of a product's lifecycle, whereas GMP is focused on production and process:

- GLP – applies to non-clinical laboratory safety studies and experiments to ensure they are high quality, reliable, consistent, and reproducible.
- GMP – applies to the manufacturing, testing, and batch-release phases of a product's lifecycle.

An Overview of Lab IT GMP Compliance

The FDA's 21 CFR Part 11 and the EU's Annex 11 can be used as guidelines for lab IT GMP compliance. The FDA's new Computer Software Assurance (CSA), and the traditional Computer Software Validation approach, can also be used as guidance when putting in place processes to ensure GMP compliance for laboratory IT infrastructure and systems.

As an overview, all computerised systems in your lab need to be validated with relevant documentation that demonstrates intended use suitability. A computerised system can be anything within your IT infrastructure, so covers PCs, software, servers, and cloud services, as well as things like SOPs (standard operating procedures), backup and archiving processes, and performance monitoring.

While all computerised systems need to be validated to ensure GMP compliance, the approach to validation should be risk-based. As a result, the validation process will differ depending on the assessed risk of the computerised system.

Importantly, the computerised system can't be viewed in isolation, as your organisation's IT infrastructure also has a role to play. Here are some examples from the ISPE GAMP Good Practice Guide that should be considered:

- The validation status of computerised systems can be compromised if its underlying IT infrastructure is not maintained in a "demonstrable state of control and regulatory compliance".
- IT infrastructure can also impact data integrity in a way that impacts patient safety and product quality.
- Your IT infrastructure needs to conform with your already established standards.

Risk considerations include the impact on product quality, patient safety, and data integrity. The complexity of the system is also an important consideration. The approach taken to validate a computerised system can also differ depending on whether a software application is off-the-shelf, customised, or custom-built.

Taking a risk-based approach to GMP compliance reduces the cost of compliance and makes the process less resource and time intensive.

Important Considerations for GMP Compliance of Lab IT Infrastructure and Systems

IQ and OQ

- Installation qualification – is the system installed and configured correctly?
- Operational qualification – is the system performing correctly according to its intended use?

Evidence

Producing and maintaining validation and qualification documentation is an essential part of GMP. Change control records should be included in validation documentation, and test methods and scenarios should be documented.

Service Providers, Suppliers, Vendors and Service Level Agreements

It is important to consider the competence and reliability of IT service providers, suppliers, and vendors, and Service level Agreements should be put in place.

Data Storage

There should be checks on data that is created, processed, and/or updated by computerised systems, including checking that data is not altered if it is transferred to another format or system.

Checking the accuracy of data is particularly critical, especially where inaccurate data can lead to high-risk scenarios.

The storage of data is also important, especially in terms of security, readability, and accessibility. Furthermore, backups should be regularly taken with the integrity and accuracy of data checked periodically.

Backup, Restore and Disaster Recovery.

The backup, restore, and archiving capability of data on any computer platform is essential to preserve the integrity of information in case of system failures.

Archiving

Archiving ensures the long-term availability of data by the provision of safe storage, indexing, and refresh activities.

Change Control

Changes to system configurations should be controlled with defined procedures.

Security

Computerised systems should be secure with [appropriate cybersecurity and access control procedures](#) and systems to protect them from unauthorised access.

Support with Lab IT GMP Compliance

At Westbourne IT, we can provide support to ensure compliance with GMP. This includes practical support in all the areas outlined above, as well as training and GMP consultancy services. To find out more, please contact us and a member of our team will get back to you.