A Basic Overview: Meeting the PIC/S Requirements for a Computerized System

Lynn Archambault
Waters Corporation, Milford, MA, USA

INTRODUCTION

The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (jointly referred to as PIC/S) provides good manufacturing practice (GMP) guidance for the lifecycle of a product. Following a brief high-level overview of GMP, this whitepaper provides a summary of the impact of PIC/S, and compliance with the PIC/S document PE 009-12 "Guide to Good Manufacturing Practice for Medicinal Products Annexes" Annex 11 Computerised Systems. It includes a high-level foundation to understand how pharmaceutical manufacturing companies are being regulated, what PIC/S means for common requirements across different countries, and how these requirements relate to meeting the expectations for data from computerised systems/electronic records.

GOOD MANUFACTURING PRACTICES

Good Manufacturing Practices are commonly referred to as GMP; sometimes the term GxP is used because there are a number of "good practices". For example, in addition to GMP, there is GCP (Good Clinical Practices), and GLP (Good Laboratory Practices). Basically the "x" in GxP represents any of these 'Good Practices' that a company should follow as they apply.

GMP is important for manufacturers of active pharmaceutical ingredients (APIs), finished pharmaceuticals, or companies that provide research and clinical trial services to such manufacturers. Figure 1 shows a high level overview of a typical manufacturing process producing finished product from raw material (note: some companies may have only a part of the process, such as producing active pharmaceutical ingredients (APIs) or excipients from raw materials). There will be a facility, which receives raw materials, the raw materials go through

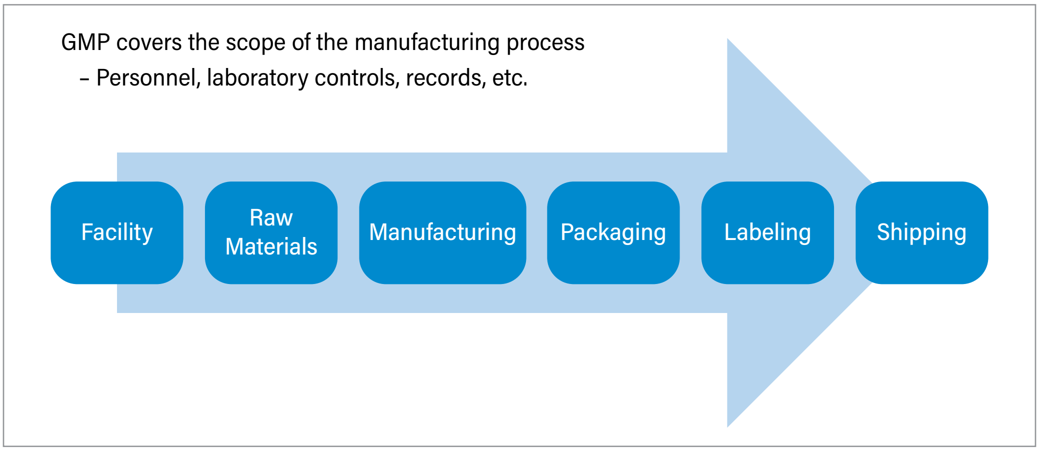

GMP covers the scope of the manufacturing process
– Personnel, laboratory controls, records, etc.
Facility
Raw Materials
Manufacturing
Packaging
Labeling
Shipping

Figure 1. Good Manufacturing Practices (GMP)

a manufacturing process, and the finished product is packaged, labeled, and shipped. There should be clear Standard Operating Procedures (SOPs) that outline the entire process from receipt of raw materials to distributing the final product to wholesalers. Using SOPs provides confidence that all steps in the process are consistent and repeatable so that the product is always the same. Within a manufacturing site, there will be a Quality Control (QC) laboratory, whose job is to produce scientific data supporting the quality of the product throughout the process. The goal is for the product to be the proper strength, identity, safety, purity, and quality each and every time the product is manufactured; regardless of location, personnel, date, or time. This data also provides information on whether or not the manufactured product is acceptable for a patient to use. It is extremely important to ensure that the data is complete, accurate, and consistent (data integrity) so the correct decision can be made about the product for the safety of the patient. Data used for these decisions can be called critical data; data in a computerised system is referred to as electronic records.

The PIC/S GMP Guide (PE 009-11, March 2014) lays out the requirements for every step of the manufacturing process from raw material receipt through distribution, and provides specific guidance for different types of products: e.g. blood and plasma and veterinary medicines. This white paper will focus on Annex 11 computerised systems and Annex 15 Qualification and Validation.

PIC/S

Pharmaceutical Inspection Convention was established in 1970. On November 2, 1995, it was merged with the Inspection Cooperation Scheme to create what's now known as PIC/S. Figure 2 shows the mission of PIC/S. PIC/S' mission is: "to lead the international development, implementation and maintenance of harmonized GMP standards and quality systems of inspectorates in the field of medicinal products." Only a regulatory agency can become a member of PIC/S if they wish to join and meet certain requirements. PIC/S' goal is to share information between regulatory agencies so that all regulated companies are inspected to the same standard. The regulatory agencies within PIC/S, such as the Taiwan Food and Drug Administration (TFDA), can share information, potentially meaning less duplicate inspections could occur for an individual company resulting in more companies being inspected, which is a benefit for the public. The intention is the higher standards and better use of inspection resources will result in safer products for patients worldwide. Shared information between regulatory bodies can include GMP compliance, inspection reports and notes, corrective actions, company plan, and follow-up letters. It's a way to harmonize resources and to make sure everyone understands what the minimum requirements are.

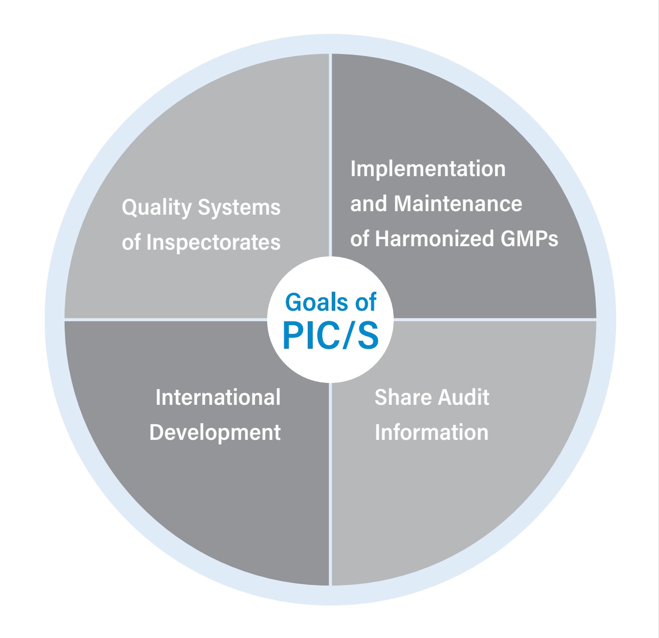

Quality Systems of Inspectorates
Implementation and Maintenance of Harmonized GMPs
Goals of PIC/S
International Development
Share Audit Information

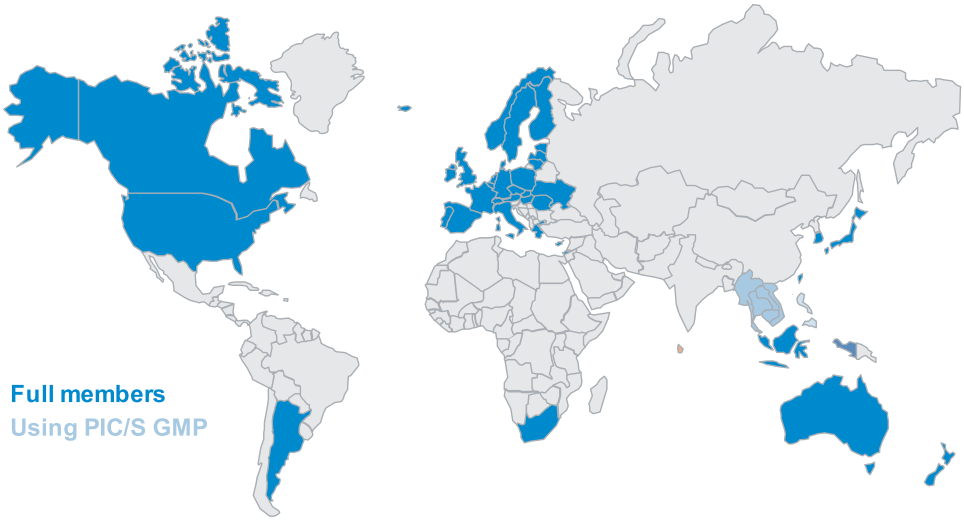
Figure 2. Goals of PIC/S

However, it is very important to understand that PIC/S is not a regulatory body itself so it does not have any inspectors, it does not control any local government regulatory body, and it does not issue GMP certificates of compliance. A member of PIC/S that is a regulatory body, such as the Japanese Pharmaceuticals and Medical Devices Agency (PMDA), issue a certificate of compliance. So, if a company passes a PIC/S inspection from one of the PIC/S members, it might mean that another regulatory body will decide not to inspect that company.

Likewise if a manufacturing facility meets PIC/S requirements for GMP, then an application for product approval in a PIC/S country is more likely to succeed because it's already met those requirements.

There is a PIC/S review process for any regulatory body that wishes to join, and certain things that a regulatory body has to have in place in order to become a member. It needs to have a law for medicine safety, it needs to have a GMP Guide (either the PIC/S GMP Guides or its own, of the same high standards of safety and quality), a regulatory inspection agency meeting PIC/S standards to audit manufacturing companies against GMPs, and it has to have experienced GMP inspectors. There are 46 Participating Authorities who are part of PIC/S as of December 2015. Figure 3 illustrates an overview on a world map with full member countries highlighted in dark blue, and in light blue, the countries that are using PIC/S GMP even though they are not full members. Many of the PIC/S countries that are on the rich end of the scale are compliant to PIC/S GMP. Consequently it's essential for a manufacturing company to be compliant with PIC/S GMP to provide them the opportunity to sell their products into these more wealthy markets. PIC/S membership is very common with most countries in the Asia-Pacific region utilizing a version of the PIC/S documents. While not all Asia-Pacific region countries have the highest Gross Domestic Product (GDP), they do have very large populations and healthcare spending by country is increasing rapidly.

China has recently released its own regulation on Computer Systems, which has much in common with the PIC/S requirements for computerised systems. But it's important to know that there are some differences. The Chinese FDA has started initial talks with the PIC/S organization about planning for membership, but not all of the countries in this region utilizing these GMP standards are currently seeking membership.



Regulatory agencies can be full members but still follow their country GMP e.g. USA

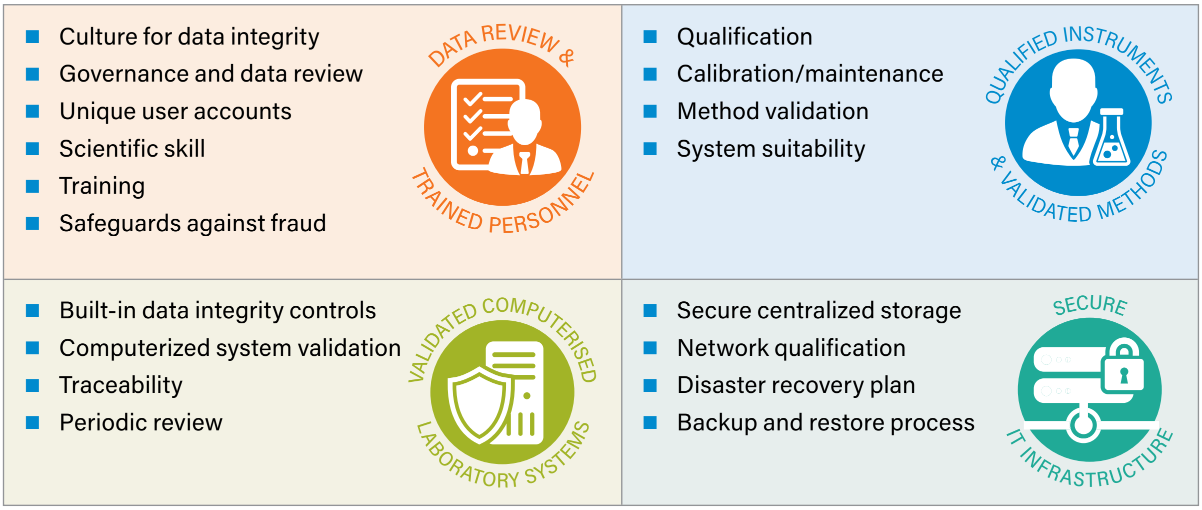
Figure 3. PIC/S members worldwide

ELECTRONIC RECORD COMPLIANCE

The combined PIC/S Annexes have a revision date of October 2015, although the text in Annex 11 hasn't changed since October 2011 and is not expected to change again anytime soon. Annex 11 covers computerised systems and must be followed by all pharmaceutical companies using computerised systems as part of their regulated process. Another important document, 'Good Practices for Computerised Systems in Regulated "GxP" Environments' (PI 011-3), is a guide for inspectors on how to audit computerised systems. This document is much older but is still valid in PIC/S and companies are encouraged to review this document. Both of these documents, Annex 11 and PI 011-3, as well as all of the applicable GMP documents, are available to download on the PIC/S website http://www.picscheme.org/

Manufacturing processes need to be designed to be reliable and consistent so the same high quality product is produced every time. The same is true for computerised systems, where the data needs to be consistent, complete and accurate at all times. It's not just about the computer though; there are computer hardware, software (the application), IT networks, analytical instruments, and of course people all interacting together and all need to be controlled to achieve compliance. Compliance builds confidence internally and externally that the data is reliable, and that it can be trusted to ensure the right strength, identity, safety, purity, and quality of a product for a patient.

Poorly controlled systems could mean a non-conformance or even worse a product that is unsafe is released and causes harm to a patient. As illustrated in Figure 4 compliance requirements for system components can be broken down into four separate components: people, analytical instruments, laboratory computerised systems, and IT components, and each of these four components require SOPs. In addition to SOPs a company can have additional resources for information such as work instructions, manuals, or technical guides to supplement the SOPs. All documents should be well controlled, documented, and managed, and personnel need to be adequately trained on the SOPs and documents that apply to their job role.



- Culture for data integrity
- Governance and data review
- Unique user accounts
- Scientific skill
- Training
- Safeguards against fraud

- Qualification
- Calibration/maintenance
- Method validation
- System suitability

- Built-in data integrity controls
- Computerized system validation
- Traceability
- Periodic review

- Secure centralized storage
- Network qualification
- Disaster recovery plan
- Backup and restore process

Figure 4. Compliance for system components

Regarding the "people" component, every company must encourage a culture for data integrity where people are rewarded for honesty; reporting a failing result is a good thing and never a cause for punishment. Everyone working together to protect the quality of the product and the safety of the patient, even more than focusing on profit and throughput are cornerstones of a data integrity culture. Data integrity governance and data review should be promoted by senior management, and the data reviews performed by skilled personnel who are actively looking to find any problems within the data. Unique user accounts should also be provided with unique passwords that are not shared. Scientific staff should be recruited with the right education and skills for the job. All users must be trained for the job they do, and how to use the computerised system, with training records documented, managed, and controlled. Safeguards against fraud should also be considered because the best way to stop data falsification or deletion is to take away most of the opportunities to do it, and then to actively search for fraud on an ongoing basis.

In addition to people, instrument qualification, including Installation, Operational, and Performance Qualification, is another important component of system compliance because it proves increased confidence that the instrument will provide reliable data to be used for decisions. Instrument compliance also includes calibration and maintenance (without these, the instrument cannot continue to provide reliable data), method validation (the method has been proven to be robust, reliable and accurate even with an amount of variation in the product due to the manufacturing process), and system suitability (using specific injections to assess if the system is functioning as expected so the results of the analysis can be used for decisions).

Laboratory computerised systems are also an important component of system compliance, including built-in data integrity controls (system features to control which users can do what actions), computerised system validation (computer system validation or CSV supports the hardware and software combination should reliably perform its intended use), traceability (traceability of system documentation shows the system is controlled, and traceability of results via an audit trail to show the history of the data), and periodic review (periodic reviews are needed to ensure that the system is still in a validated state and continues to operate according to GMP requirements). Periodic reviews are like an 'internal audit' on the system to make sure that changes over time to software versions, people, and processes have all been controlled and did not take the system out of compliance.

Finally IT Components must be considered as a part of system compliance. Secure centralized storage where all of the data is kept in a single, secure location that is backed up and cannot be accessed except by authorized IT administrators. Long term, the data can be archived from the live system to some offline storage – but the capability to restore it back into the system when it's needed for an audit or investigation must exist.

Network qualification; testing to make sure the network can handle the use and storage of data to meet the company needs. A disaster recovery plan, or how to recreate the computerised system (including instruments) and restore the data to get running again after a major disaster must also be considered. A backup and restore process, that is periodically tested, will ensure that data can be restored from backed-up data from a centralized storage facility in case of a failure.

What When	QUALIFIED INSTRUMENTS & VALIDATED METHODS	VALIDATED COMPUTERISED LABORATORY SYSTEMS	SECURE IT INFRASTRUCTURE
Considerations During Project Planning	Compatibility with chosen CDS* or LIMS* or other critical software	Software provider may be separate to hardware provider	IT may be in-house or external; SLA* always needed
Vendor Assessment Before Purchase Order Placement	The need for Vendor Assessment (audit) on an external vendor will be based on a Risk Assessment, and the scope of any such audit should be: *Quality Management System, Development Lifecycle, Product and Supplier Maturity*		
Service Level Agreements Throughout Operational Life	Maintenance contract	Installation, software upgrades, ongoing support	Response time, Maximum downtime, virus and patches

**CDS = Chromatography Data System; LIMS = Laboratory Information Management System; SLA = Service Level Agreement*

Figure 5. Purchased components

VENDOR ASSESSMENTS

Something else to consider when buying an instrument, a computerised system, or outsourcing IT, is performing a vendor assessment as recommended by PIC/S Annex 11 following a risk assessment to determine need. As highlighted in Figure 5, any vendor assessment should be documented, and if any non-conformances are observed, the vendor should complete any corrective actions before any orders are placed. Instruments should be compatible with any other systems; e.g. HPLC instruments should be compatible with the existing chromatography data system, and maintenance contracts should be considered to keep the instrument calibrated. Well maintained instruments increase the confidence that the data obtained from them is reliable.

For computerised systems, it is important to make sure what hardware is supplied. A service level agreement should also be used to make sure ongoing support, including software upgrades, can be provided. The entire process and all parties who are associated from the start, including the vendor and IT, all need to be well aligned and understand what their responsibilities are to help satisfy Annex 11 requirements. Additional details are provided.

INSPECTING FOR DATA INTEGRITY

Inspectors are focused on data integrity: is the data complete, consistent and accurate throughout the entire life cycle of the data-creation through the retention period until the point when it's acceptable for it to be destroyed. It's very important to understand that it is no longer acceptable to keep printed chromatograms as a record. All electronic data including the metadata needs to be retained, the chromatogram alone doesn't specify the processing information, or how it was acquired, which is why the electronic record needs to be retained to understand the whole story. Data integrity includes both the good and the bad results, because inspectors want to understand not just how a company deals with all the good information (that process is usually very straightforward), but how a company assesses and deals with the mistakes, the deviations, and the issues and problems, an indication that the company is well controlled.

Metadata, the behind-the-scenes acquisition and processing information, are important to understanding how that data was collected and how results are calculated. The regulatory agencies will use the term 'ALCOA' when they talk about data integrity: short for Attributable, Legible, Contemporaneous, Original, and Accurate. Information needs to be Attributable, as in knowing who acquired the data or performed the action. It needs to be Legible, so that the data entries can be read and easily understood. It needs to be Contemporaneous, or documented at the time of the activity. It needs to be Original, or the first recording observation. It needs to be Accurate, so there's no errors or editing performed. ALCOA can also be extended to include Complete (all data including any repeat or reanalysis performed), Consistent (all elements of the analysis, such as the sequence of events, follow on and are dated or time stamped in expected sequence), Enduring (recorded in a permanent, maintainable form for the useful life), and Available (for review and audit or inspection over the lifetime of the record).

There are currently several areas of regulatory concern worldwide that inspectors are likely to focus on. They include:

- Computerised system that are not validated.
- Insufficient controls over access and privileges, to make sure that laboratory personnel are not able to delete data.
- Inappropriate use of uncontrolled and undocumented trial injections.
- Renaming files to falsely apply them to other samples (this situation can happen when flat file structures are used rather than relational databases which provide traceability).
- Use of local hard drives with poor or manual back-up processes instead of secure servers with automated back-up and archiving enabled.

CONCLUSION

PIC/S provides an opportunity to comply with a single GMP and access many target countries. Passing an inspection from a PIC/S member regulatory agency may reduce the number of future inspections and open up new export markets. For computerised systems, it's the whole environment that needs to be compliant: including the hardware, software, people, instruments, and processes. Together this compliance will provide data integrity, and the knowledge that the data used to keep patients safe can be trusted.

COMPLIANCE TOOLS FROM WATERS

Waters has several different compliance-ready products such as:

- The Empower® 3 Chromatography Data System
- UNIFI® Scientific Information System
- NuGenesis® Laboratory Management System.

In addition, Waters offers many professional services including: training, and maintenance and validation consulting, as well as a large library of supporting compliance literature.

Waters

THE SCIENCE OF WHAT'S POSSIBLE.®

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
www.waters.com