WORLD JOURNAL OF PHARMACEUTICAL RESEARCH
SJIF Impact Factor 8.074
Volume 8, Issue 10, 618-629. Review Article ISSN 2277– 7105

OVERVIEW OF REGULATIONS ON GMP COMPUTERIZED SYSTEMS

D. Chandra Sai*

Manager-QA (Computer System Validation), Gland Pharma Ltd, Hyderabad, Telangana.

Article Received on
07 July 2019,

Revised on 28 July 2019,
Accepted on 18 August 2019,

DOI: 10.20959/wjpr201910-15718

***Corresponding Author**
D. Chandra Sai
Manager-QA (Computer System Validation), Gland Pharma Ltd, Hyderabad, Telangana.

ABSTRACT

During the manufacturing and testing of the pharmaceutical products firms uses different automated solutions at various manufacturing steps. In recent times automation and digitalization playing a big role in the industry from development to distribution of product to patient. Computer or related systems and electronic records vastly involve in the pharmaceutical manufacturing process. There are certain guidelines established from different global regulatory bodies to ensure the manufacturing and testing of drug products using computerized process is appropriate and equal to controlled manual process. Complying with these guidelines or requirements is more crucial for each pharmaceutical firm to get approval to market the drug products to respective regions.

KEYWORD: Predicate rules, 21 CFR Part 211, 21 CFR Part11, EU Annex 11, computerized system, Electronic records.

INTRODUCTION

US Foods and Drugs Administration department (US FDA) is a major regulatory among all pharmaceutical regulators in the globe. There are multiple numbers of regulations designed by the FDA for each industry such as pharmaceutical, clinical, food, cosmetics. For FDA pharmaceuticals industry is more considerable to control and monitor the quality manufacturing. There are certain predicate rules established for a computer or related systems i.e. 21 CFR Part 211.68 and 21 CFR Part 11 will be applicable where electronic records and electronic signatures generated under predicate requirement. Apart from FDA, the European Commission has published Annex 11 guidelines for computerized systems and electronic records. ICH issued technical requirements on computerized system PIC/S released guidance document on GxP computerized systems. Along with these longstanding rules all major

regulatory bodies set forth data integrity requirements in recent times which are majorly applicable to electronic records and computerized systems. This article will summarize foremost regulations applicable to a computer or related systems including electronic records and signatures.

Predicate rules

A predicate rule is one that which is outlined in the US Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act or any FDA regulation (GxP: GLP, GMP, GCP, etc.).

Computer or related systems

Computer or related systems can refer to computer hardware, software, peripheral devices, networks, cloud infrastructure, personnel, and associated documents (e.g., user manuals and standard operating procedures).

Computerized system

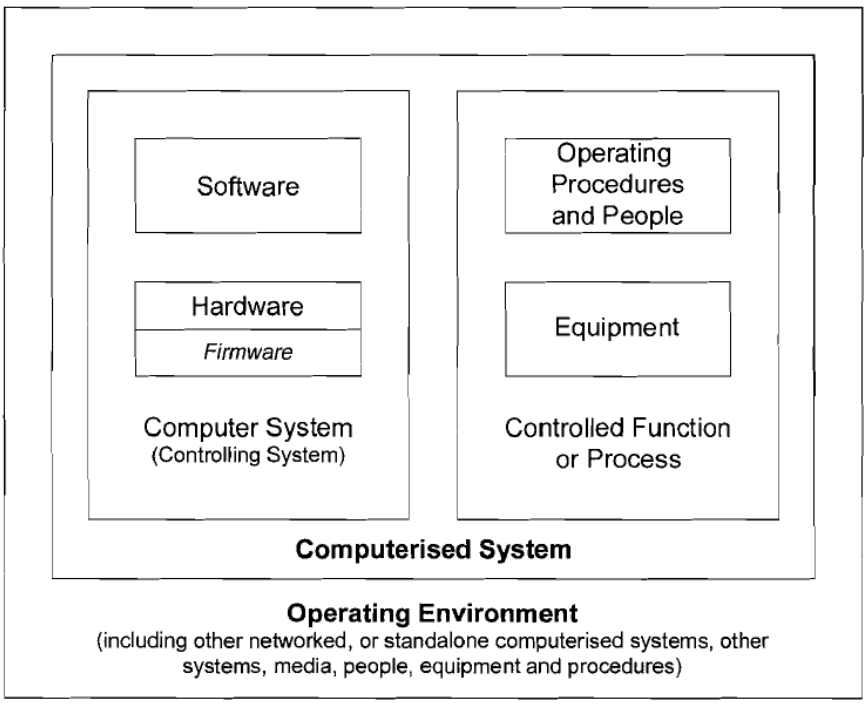

Fig 1: Computerized system-From GAMP 5 guidance document.

Electronic records

Records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements outlined in agency regulations.

Applicability of regulations to a computer or related systems

Regulations may not apply for all computer systems uses in particular pharmaceutical firm. The following questions can be used to deciding the applicability of predicate rules. If any of the following questions is "yes" then those systems can be categorized as "GxP" (GMP, GLP, GDP, etc.).

- Does the system control or execute a manufacturing/testing process that has a direct impact on product quality, strength, identity, safety & purity?
- Does the system produce data, which is used to release components or materials?
- Does the system generate information in an electronic format that is required by regulatory agencies?
- Does the system generate data feeds information to another system, which supports regulated information activities?
- Is the system used to monitor & record relevant process-related predicate rules?

Regulations on a computer(ized) or related systems

The US FDA and the European Commission provided a set of rules for a computer or related systems. Also ICH and PIC/S also published guidelines on computerized systems.

21 CFR Part 211 requirements on computer or related systems are briefly interpreted below.

Mainly there are three categories as per FDA 21 CFR part 211.68, i.e. Automatic, mechanical, and electronic. A here electronic system can be considered as a computerized system. Requirements from this predicate rules are briefly mentioned below

- Validation to ensure satisfactory functioning
- Written procedure and record to assure performance routinely
- Appropriate access control to assure the changes in records institute by authorized persons.
- Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy and this verification shall be based on the complexity and reliability of the system.
- A backup file of data entered into the computer or related system shall be maintained
- Backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained.

- Computer systems electronic records must be controlled including records retention, backup, and security.
- Based on the complexity and reliability of computer systems there must be procedural controls and technologies to ensure the accuracy and security of computer systems, I/Os, electronic records and data.
- Computer systems must have adequate controls to prevent unauthorized access or changes to data, inadvertent erasures, or loss.
- Computer electronic records must be controlled, and this includes record backup, security, and retention.
- There must be a written program detailing the maintenance of the computer system, including on-going performance evaluation and periodic reviews.
- Specifically for Sections 211.101(c), 211.103, 211.182, and 211.188(b)(11), verification by a second individual may not be necessary when automated equipment is used as described under Section 211.68.

EU Annex 11 requirements on computerized systems including electronic records and signatures briefly interpreted below

1. Risk assessment

- Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity, and product quality

2. Personnel

- All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties

3. Suppliers and Service Providers

- When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain, modify or retain a computerized system or related services, formal agreements must exist.
- The need for supplier audit should be based on a risk assessment.
- Quality system and audit information should be made available to inspectors on request.

4. Validation

- The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures, and records based on their risk assessment.

5. Data

- Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, to minimize the risks.

6. Accuracy Checks

- For critical data entered manually, there should be an additional check on the accuracy of the data.

7. Data Storage

- Data should be secured by both physical and electronic means against damage. Access to data should be ensured throughout the retention period. Regular back-ups of all relevant data should be done.

8. Printouts

- It should be possible to obtain clear printed copies of electronically stored data.

9. Audit Trails

- Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

10. Change and Configuration Management

- Any changes to a computerized system including system configurations should only be made in a controlled manner by following a defined procedure.

11. Periodic evaluation

- Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.

12. Security

- Physical and/or logical controls should be in place to restrict access to the computerized system to authorized persons.

13. Incident Management

- All incidents, not only system failures and data errors, should be reported and assessed.

14. Electronic Signature

- Electronic records may be signed electronically. Electronic signatures are expected to: have the same impact as hand-written signatures, be permanently linked to their respective record and include the time and date that they were applied.

15. Batch release

- The system should allow only Qualified Persons to certify the release of the batches.

16. Business Continuity

- Computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown.

17. Archiving

- Data may be archived. This data should be checked for accessibility, readability, and integrity.

ICH 7 guidelines on computerized systems including electronic records and signatures briefly interpreted below (5.4 Computerized systems)

1) 5.40: Validation

- GMP related computerized systems should be validated.

2) 5.41: IQ/OQ

- Appropriate installation qualification and operational qualification should demonstrate the suitability of computer hardware and software to perform assigned tasks.

3) 5.42: Reduced testing; Retrospective validation

- Commercially available software that has been qualified does not require the same level of testing. If an existing system was not validated at time of installation, a retrospective validation could be conducted.

4) 5.43: Access controls and audit trail

- Computerized systems should have sufficient controls to prevent unauthorized access or changes to data or to prevent omissions in data. Changes should be recorded.

5) 5.44: Procedures

- procedures should be available for the operation and maintenance.

6) 5.45: Additional checks

- Additional checks for manual data entry by system itself or by second person.

7) 5.46: Incident management

- Incidents related to computerized systems should be recorded and investigated.

8) 5.47: Changes management

- Changes to the computerized system should be formally authorized, documented and tested to maintain the validated state.

9) 5.48 Data protection

- Data backup policies should be established for all computerized systems to ensure data protection during breakdowns and failures.

10) 5.49 Data can be recorded by a second means in addition to the computer system.

PIC/S guidelines on computerized systems including electronic records and signatures briefly interpreted below (PI011 Good Practices for Computerized Systems in Regulated "GxP" environments)

1) Implementation of Computerized systems

- The structure and functions of the computer system(s)
- Planning and life-cycle management
- Management and responsibilities

- User requirement specifications (URS)
- Functional specifications (FS)
- Suppliers, software developers and quality management
- Important QMS and software standards attributes
- Testing Validation strategies and priorities
- GAMP validation approach based on different categories of software products
- Retrospective validation

2) System Operation

- Change management
- Change control and error report system
- System security, including back-up
- Data changes - audit trail/critical data entry
- Electronic records and electronic signatures
- Personnel

Regulations on electronic records and electronic signatures

21 CFR Part 11 regulation was released in 1997 to set forth requirements for electronic records and signatures. With FDA's early interpretation and enforcement, the industry had confusion where Part11 regulation was actually applicable. The FDA changed the approach in 2003 with the release of new guidance. The recommendation was to implement Part 11 based on predicate rule requirements and on the risk of records on product quality and data integrity. 21 CFR Part 11 requirements on electronic records and signatures briefly referred and interpreted below.

1) 11.10 (a): System must be validated and the system should able to detect invalid or altered records

- All computer systems used to generate, maintain and archive electronic records must be validated to ensure accuracy, reliability, consistent independent performance and the ability to discern invalid or altered records.

2) 11.10 (b): Electronic records must be accurate and complete in readable electronic form.

- The ability to generate accurate and complete copies of records in both human-readable and electronic form suitable for inspection, review, and copying by the agency.

3) 11.10 (c): Secure Retention of Electronic Records and Instant Retrieval

- Protection of records to enable their accurate and ready retrieval throughout the records retention period.

4) 11.10 (d): Limited access

- Limiting system access to authorized individuals.

5) 11.10 (e): secure, computer-generated, time-stamped audit trails

- Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.

6) 11.10(f): Enforcement of Permitted Sequencing

- Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

7) 11.10(g): Use of Authority Checks

- Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

8) 11.10(h): Use of Deice Checks

- Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

9) 11.10(i): Qualification of persons

- The determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

10) 11.10(j): Individual Accountability

- The determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

11) 11.10(k): System Documentation

- Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. Revision and change control procedures to maintain development and modification of systems documentation.

12) 11.30: Controls for open systems

- Procedures and controls mentioned in part 11.10 shall be established to ensure authenticity, integrity, and the confidentiality of electronic records as appropriate.
- Use of document encryption and digital signature to ensure the record authenticity, integrity, and confidentiality.

13) 11.50 Signature manifestations

- Signed electronic records shall contain information

The printed name of the signer;

The date and time when the signature was executed; and

The meaning

- Signature information should display on records in human readable form

14) 11.70 Signature/record linking

- Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records.

15) 11.100 (a): Uniqueness

- Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

16) 11.100 (b): Identity of signer

- "Before establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, the organization shall verify the identity of the individual".

17) 11.100(c): certify to the agency

- Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

18) 11.300: Controls for identification codes/passwords

- Uniqueness.
- periodically checked, recalled, or revised.
- loss management procedures.
- safeguards to prevent unauthorized use.
- Initial and periodic testing of device to ensure that they function properly and have not been altered in an unauthorized manner.

Data integrity requirements on electronic and computer or related systems

In recent times data integrity guidance documents were released by foremost regulatory bodies like USFDA, MHRA, and others. Fulfillment of these requirements certainly required to maintain data integrity and reliability. The common expectation from those guidance documents are briefly.

Electronic data must be

- A - Attributable to the person generating the data
- L – Legible and permanent
- C – Contemporaneous
- O – Original record (or ‘true copy')
- A - Accurate
- Validation of computerized systems
- Audit trail and review
- Authorized individual access
- Data retention

ACKNOWLEDGMENT

All resources of article and the persons who actually created the contents of information that provided a basis for the ideas delivered in this article are considerately acknowledged.

CONCLUSION

The overall objective of this article to indicate major applicable regulations for computerized systems and electronic records. Compliance with these regulations in the pharmaceutical industry plays a critical role to ensure appropriate validation, data integrity, authorized access, periodic review, maintenance, data backup and retrieval, vendor assessment, business continuity. Each pharmaceutical manufacturer shall have appropriated procedures to implement applicable controls to assure the right manufacturing or testing or packing process to produce quality products to the consumer.

REFERENCES

1. Title 21--Food and Drugs Chapter I--Food and Drug Administration Department Of Health and Human Services Subchapter C--Drugs: General Part 211 Current Good Manufacturing Practice For Finished Pharmaceuticals.
2. Title 21--Food and Drugs Chapter I--Food and Drug Administration Department of Health and Human Services Subchapter A—General Part 11 Electronic Records; Electronic Signatures.
3. GAMP 5 - A risk based approach to compliant GxP computerized system.
4. EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines-Annex 11.
5. pharmacentral.in/wp-content/uploads/2019/04/13-Risk-assessment-CSV.pdf- Louise Morris.
6. https://www.labcompliance.com/info/links/fda/regulations.aspx.
7. https://www.slideshare.net/tonysteinberg/interpretation-of-part-11-by-the-gxp-predicate-rules.
8. Journal of GXP Compliance-Orland Lopez.
9. US FDA Data Integrity and Compliance with Drug CGMP Questions and Answers Guidance for Industry, December 2018.
10. MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015.
11. Data Integrity: TGA Expectations - Stephen Hart, Senior Inspector, Manufacturing Quality Branch, TGA, PDA conference July 2015.
12. Q7-ICH: https://www.ich.org/fileadmin/Public_Web_Site/ICH.../Q7/Step4/Q7_Guideline.pdf
13. Pharmaceutical Inspection Convention pharmaceutical Inspection Co-Operation Scheme PI 011-3, 25 September 2007.