NORMATIVE INSTRUCTION (IN) No. 134 OF 30 MARCH 2022

Provides for the Good Manufacturing Practices complementary to computerized systems used in the manufacture of medicinal products.

The Collegiate Board of Directors of the Brazilian Health Regulatory Agency, in the use of the attributions vested in it under Article 15, items III and IV, and Article 7, item III of Law no. 9,782 of 26 January 1999, and item VII, paragraphs 1 and 3 of Article 187 of the Internal Regulation approved by Collegiate Board Resolution – RDC no. 585 of 10 December 2021, adopts the following Normative Instruction, as decided upon in the Extraordinary Meeting – RExtra 6, held on 30 March 2022, and I, Director-President, determine its publication.

CHAPTER I

INITIAL PROVISIONS

Section I

Objective

Article 1. This Normative Instruction has the objective of adopting the guidelines on Good Manufacturing Practices related to the computerized systems of the Pharmaceutical Inspection Cooperation Scheme (PIC/S), as complementary requirements to be followed in the manufacture of medicinal products in addition to the General Guidelines on Good Manufacturing Practices for Medicinal Products.

Section II

Scope

Article 2. This Normative Instruction applies to all forms of computerized systems used as part of activities regulated by the Good Manufacturing Practices for medicinal products, including experimental medicines.

Section III

Definitions

Article 3. For the purposes of this Normative Instruction, the following definitions are adopted:

I – application: software installed on a defined platform/ hardware, providing a specific functionality;

II – life cycle: all phases of system life, from initial requirements to decommissioning, including design, specification, programming, testing, installation, operation, and maintenance;

III – IT infrastructure: the hardware and software, such as network software and operating systems, that make it possible for the application to function;

IV – business: object to be studied in validation, it comprises data and material management, analytical activities, production process, etc.;

V – process owner: the person responsible for the process of the business;

VI – system owner: the person responsible for providing and maintaining a computer system and for the security of the data residing in that system;

VII – customized or tailored computer system: a computer system individually designed to fit a specific business process;

VIII – commercial off-the-shelf software: commercially available software whose suitability for use is demonstrated by a wide range of users; and

IX – third party: parts not managed directly by the holder of the manufacturing or import authorization.

CHAPTER III

GENERAL PROVISIONS

Section I

Introduction

Article 4. A computer system is a set of software and hardware components that together fulfill certain functionalities.

Article 5. The application must be validated.

Article 6. The information technology infrastructure must be qualified.

Article 7. Whenever a computerized system replaces a manual operation, there must be no decrease in product quality, process control, quality assurance, or an increase in overall risk to the process.

Section II

Risk Management

Article 8. Risk management must be applied during the entire life cycle of the computerized system, taking into consideration patient safety, data integrity, and product quality.

Article 9. Decisions on the extent of data integrity validation and control must be based on and justified by documented risk assessments of the computerized system.

Section III

Personnel

Article 10. The Process Owner, System Owner, Authorized Persons, IT and other relevant areas and persons must have appropriate qualifications, level of access, and defined responsibilities to perform their duties.

Section IV

Suppliers and Service Providers

Article 11. When suppliers, service providers, or other third parties are used to supply, install, configure, integrate, validate, maintain, modify, or store a computer system or related service, or for data processing purposes, contracts must exist between the manufacturer and any third parties, with clear statements of the third party's responsibilities.

Sole paragraph. The information technology departments of the contracting party and the contracted party must be considered analogous.

Article 12. The competence and reliability of a supplier are considered essential elements during product or service provider selection, and the need to determine them by means of an audit must be established by a documented risk assessment.

Article 13. Documentation presented with commercial off-the-shelf software must be reviewed by qualified users to verify whether user requirements are met.

Article 14. Information about the quality management systems and about audits carried out on suppliers or developers of software and implemented systems must be made available to inspectors whenever requested.

CHAPTER III

SPECIFIC PROVISIONS

Section I

Validation of the Design Phase

Article 15. Validation documents and reports must cover the relevant life cycle steps.

Article 16. Manufacturers must justify their standards, protocols, acceptance criteria, procedures, and records based on their risk assessment.

Article 17. The validation documentation must include records of alteration controls and investigation reports of any deviations observed.

Article 18. An inventory of all relevant systems and functionalities related to the Good Manufacturing Practices must be maintained by the company and made available upon request.

Article 19. Up-to-date descriptions of critical systems must be available, detailing the physical and logical arrangements, data flows, and interfaces with other systems or processes, any hardware and software prerequisites, and security measures.

Article 20. The specifications of user requirements must describe the functions required of the computerized system and be based on a documented risk assessment as well as on the impact on the Good Manufacturing Practices.

Sole paragraph. User requirements must be traceable throughout the life cycle.

Article 21. The user must take the relevant measures to ensure that the system has been developed in accordance with an appropriate quality management system.

Sole paragraph. The system supplier must be evaluated adequately.

Article 22. For the validation of customized or tailored computerized systems, there must be a process that ensures the formal evaluation and recording of quality and performance measures for all stages of the system's life cycle.

Article 23. Evidence of appropriate test methods and scenarios must be demonstrated.

Paragraph 1. The evidence referred to in the caption of this article must include system (process) parameter limits, data limits, and error handling.

Paragraph 2. Automated test tools and test environments must have documented assessments of their suitability.

Article 24. If data are transferred to another data format or system, validation must include checks that data value or meaning have not been altered during such migration process.

Section II

Operational Phase

Subsection I

Data

Article 25. The exchange of electronic data from computerized systems with other systems must have appropriate coupled checks for correct and secure data feeding and processing, in order to minimize risks.

Subsection II

Accuracy Checks

Article 26. For critical data manually entered, there must be an additional check on data accuracy.

Paragraph 1. The verification referred to in the caption of this article may be made by a second operator or by validated electronic means.

Paragraph 2. The criticality and potential consequences of erroneous or incorrectly entered data in a system must be covered by the risk assessment.

Subsection III

Data Storage

Article 27. The data must be protected by physical and electronic means against damage.

Article 28. The stored data must be checked for accessibility, readability, and accuracy.

Article 29. Access to stored data must be ensured during the entire storage period.

Article 30. All relevant data must be backed up.

Sole Paragraph. The integrity and accuracy of backup data and the ability to restore data must be verified during validation and periodically monitored.

Subsection IV

Prints

Article 31. The electronically stored data must enable the generation of clear hard copies.

Article 32. For the records that support the release of batches, it must be possible to generate printouts indicating whether any of the data has been altered since their original insertion.

Subsection V

Audit Trails

Article 33. Based on risk analysis, the construction of an audit trail system of all relevant deletions or alterations relevant to the Good Manufacturing Practices must be considered.

Paragraph 1. For alteration or deletion of data relevant to the Good Manufacturing Practices, reasoning must be documented.

Paragraph 2. Audit trails must be available and must be capable of being presented in an understandable format when made available.

Paragraph 3. Audit trails must be reviewed regularly.

Subsection VI

Alteration Management and Configuration Management

Article 34. Any alterations to a computer system, including system settings, must be made in a controlled manner, according to a defined procedure.

Subsection VII

Periodic Evaluation

Article 35. Computerized systems must be periodically evaluated to confirm that they remain validated and in compliance with the Good Manufacturing Practices.

Sole Paragraph. The evaluations referred to in the caption of this article must include, when appropriate, the current set of functionalities, deviation logs, incidents, problems, update history, performance, reliability, security, and validation status reports.

Subsection VIII

Security

Article 36. Physical or logical controls must be in place to ensure that access to the computer system is allowed only to authorized persons.

Sole Paragraph. Appropriate methods to prevent unauthorized access to the system may include the use of keys, access cards, personal codes with passwords, biometric data, restricted access to computer equipment, and data storage areas.

Article 37. The extent of security controls must be determined according to an assessment of the criticality of the computer system.

Article 38. The creation, alteration, and cancellation of access authorizations must be recorded.

Article 39. Data and document management systems must be designed to record the identity of users who enter, alter, confirm, or delete data, including date and time.

Subsection IX

Incident Management

Article 40. All incidents, not only system failures and data errors, must be logged and assessed.

Sole paragraph. The root cause of critical incidents must be identified and form the basis of corrective and preventive actions adopted.

Subsection X

Electronic Signature

Article 41. Electronic records may be signed electronically.

Article 42. Electronic signatures must:

I – have the same impact as handwritten signatures within the boundaries of the company;

II – link permanently to its respective register;

III – include the time and date when they were applied; and

IV – for records used externally, the electronic signature must meet the locally applicable digital certification guidelines.

Subsection XI

Batch Release

Article 43. When a computerized system is used for batch release, it must be ensured that only the Person Delegated by the Pharmaceutical Quality System has permission to such functionality.

Paragraph 1. A record specifying the person responsible for the release referred to in the caption of this article must be available.

Paragraph 2. The identification and registration of the responsible person must be done by means of an electronic signature.

Subsection XII

Business Continuity

Article 44. There must be measures in place to ensure the continuity of critical processes in case of failure of the computerized systems that support them, such as alternative systems or manual records.

Paragraph 1. The time needed to put such alternative measures in place must be risk-based, and appropriate for a given system and the supported business process.

Paragraph 2. The alternative measures referred to in Paragraph 1 of this article must be adequately documented and tested.

Subsection XIII

Filing

Article 45. Data may be archived as long as they remain accessible, legible, and complete.

Sole paragraph. If relevant changes to the system are required, the ability to recover the data must be ensured and tested.

CHAPTER IV

FINAL PROVISIONS

Article 46. Non-compliance with the provisions contained in this Normative Instruction constitutes a health infraction, pursuant to Law no. 6,437 of 20 August 1977, without prejudice to the applicable civil, administrative, and criminal liabilities.

Article 47. Normative Instruction – IN No. 43 of 21 August 2019 is hereby revoked.

Article 48. This Normative Instruction enters into force on 2 May 2022.

ANTONIO BARRA TORRES