Health Canada Santé Canada

Your health and safety… our priority. *Votre santé et votre sécurité… notre priorité.*

Annex 11 to the Good manufacturing practices guide – Computerized Systems

GUI-0050

August 10, 2021

Canada

Date issued:	August 10, 2021
Date implemented:	August 10, 2021
Replaces:	PIC/S Annex 11: Computerised Systems (April 5, 2007)

Health Canada is the federal department responsible for helping the people of Canada maintain and improve their health. Health Canada is committed to improving the lives of all of Canada's people and to making this country's population among the healthiest in the world as measured by longevity, lifestyle and effective use of the public health care system.

Également disponible en français sous le titre :
Annexe 11 aux lignes directrices sur les bonnes pratiques de fabrication – systèmes informatisés

For more information, please contact:

Health Canada
Address Locator 0900C2, Ottawa, ON K1A 0K9
Tel.: 613-957-2991
Toll free: 1-866-225-0709
Fax: 613-941-5366
TTY: 1-800-465-7735
Email: publications@hc-sc.gc.ca

This publication can be made available in alternative formats upon request.

Publication date: August 2021

Cat.: H139-18/2020E-PDF
ISBN: 978-0-660-35745-4
Pub.: 200161

Disclaimer

This document does not constitute part of the *Food and Drugs Act* (the Act) or its regulations and in the event of any inconsistency or conflict between the Act or regulations and this document, the Act or the regulations take precedence. This document is an administrative document that is intended to facilitate compliance by the regulated party with the Act, the regulations and the applicable administrative policies.

Table of contents

About this document 5
1. Purpose 5
2. Scope 5
3. Introduction 6

General 7
4. Guidance 7
4.1. Risk Management 7
4.2. Personnel 7
4.3. Suppliers and Service Providers 7

Product Phase 8
4.4. Validation 8

Operational Phase 9
4.5. Data 9
4.6. Accuracy Checks 10
4.7. Data Storage 10
4.8. Printouts 10
4.9. Audit Trails 10
4.10. Change and Configuration Management 10
4.11. Periodic Evaluations 11
4.12. Security 11
4.13. Incident Management 11
4.14. Electronic Signature 11
4.15. Batch Release 12
4.16. Business Continuity 12
4.17. Archiving 12

Appendices 13
Appendix A – Glossary 13
Acronyms 13
Terms 13
Appendix B – References 15

The following is the type of icon used in this document, and the way it is intended to be used.

Information: Supplementary information like quotes and legal references.

About this document

1. Purpose

This annex applies to all forms of computerized systems used as part of Good Manufacturing Practices (GMP) regulated activities. A computerized system is a set of software and hardware components which together fulfil certain functionalities.

The application should be validated; Information Technology (IT) infrastructure should be qualified.

Where a computerized system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

This guidance document is an annex to the current edition of the *Good manufacturing practices guide for drug products (GUI-0001)*. Definitions of terms used in this guide can be found under Appendix A.

The guidance that follows has been adopted from "Annex 11: Computerised Systems" in the Pharmaceutical Inspection Cooperation Scheme (PIC/S) document *Guide to good manufacturing practice for medicinal products annexes (PE-009-15)*.

Please note that although this is a direct adoption of PE-009-15, some PIC/S terms have been replaced with Canadian terms to reflect the terminology used in Health Canada.

2. Scope

These guidelines apply to the following product categories:

- pharmaceutical
- radiopharmaceutical
- biological
- veterinary

3. Introduction

These guidelines interpret the requirements for good manufacturing practices (GMP) in Part C, Division 2 of the Food and Drug Regulations (the Regulations).

Health Canada is an active participating member of the Pharmaceutical Inspection Cooperation Scheme (PIC/S). Health Canada has adopted the PIC/S guidance Annex 11 Computerised Systems which applies to all forms of computerized systems used as a part of GMP regulated activities.

Guidance documents like this one are meant to help industry and health care professionals understand how to comply with the relevant Canadian legislations. They also provide guidance to Health Canada staff so that the regulations are enforced in a fair, consistent and effective way across Canada.

Health Canada inspects establishments to assess their compliance with the *Food and Drugs Act* (the Act) and associated regulations. When we conduct an inspection, we will use this document as a guide in assessing your compliance with GMP requirements.

These guidelines are not the only way GMP regulations can be interpreted, and are not intended to cover every possible case. Other ways of complying with GMP regulations will be considered with proper scientific justification. Also, as new technologies emerge, different approaches may be called for.

Guidance documents are administrative and do not have the force of law. Because of this, they allow for flexibility in approach. So use this guide to help you develop specific approaches that meet your unique needs.

General

4. Guidance

4.1 Risk Management

Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.

4.2 Personnel

There should always be close cooperation between all relevant personnel such as Process Owner, System Owner and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

4.3 Suppliers and Service Providers

1. When third parties (e.g. suppliers, service providers) are used to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the Drug Establishment Licence holder and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

2. The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

3. Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

4. Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

Project Phase

4.4 Validation

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

2. Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

3. An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

4. User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

5. The regulated user should take all reasonable steps to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

6. For the validation of bespoke or customised computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

7. Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

8. If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

There are multiple approaches to validation of computerized systems. You can find more information in the PIC/S *Good Practices for Computerised Systems in Regulated "GXP" Environments (PI 011-3)*. Health Canada will accept approaches such as this that are justified based on good science.

Other considerations could include:

- Health Canada's *Guide to validation – drugs and supporting activities (GUI-0029)*
- *ASTM E2500 - 13 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment*
- ISO Standards as applicable
- IEEE Standards:
    - *IEEE 729 Glossary of Software Engineering Terminology*
    - *IEEE 730 Quality Assurance Plan*
    - *IEEE 828 Software Configuration Management Plans*
    - *IEEE 829 Software Test Documentation*
    - *IEEE 830 Guide to Software Requirements Specification*
    - *IEEE 983 Guide to Software Quality Assurance Planning*
    - *IEEE 1012 Software Verification Plans*
    - *IEEE 1298 Software Quality Management System Part 1: Requirements*

Operational Phase

4.5 Data

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

4.6 Accuracy Checks

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

4.7 Data Storage

1. Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

2. Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

4.8 Printouts

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

2. For records supporting batch release, it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

4.9 Audit Trails

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

4.10 Change and Configuration Management

Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

4.11 Periodic Evaluations

Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

4.12 Security

1. Physical and/or logical controls should be in place to restrict access to computerized system to authorized users. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

2. The extent of security controls depends on the criticality of the computerized system.

3. Creation, change, and cancellation of access authorisations should be recorded.

4. Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

4.13 Incident Management

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

4.14 Electronic Signature

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,
b. be permanently linked to their respective record,
c. include the time and date that they were applied.

4.15 Batch Release

When a computerized system is used for recording certification and batch release, the system should allow only Authorized users to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

4.16 Business Continuity

For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on the risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

4.17 Archiving

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Appendices

Appendix A – Glossary

Acronyms

GMP: Good manufacturing practices

IEEE: The Institute of Electrical and Electronics Engineers Standards Association

ISO: The International Organization for Standardization

IT: Information Technology

PIC/S: Pharmaceutical Inspection Cooperation/Scheme

Terms

These definitions explain how terms are used in this document. Definitions quoted from other documents are identified in brackets at the end of the definition. If there is a conflict with a definition in the *Food and Drugs Act* or Food and Drug Regulations, the definition in the Act/Regulations prevails. More applicable definitions can be found in the *Good manufacturing practices guide for drug products (GUI-0001)*.

Application – Software installed on a defined platform/hardware providing specific functionality.

Bespoke/Customised computerized system – A computerized system individually designed to suit a specific business process.

Commercial off-the-shelf software – Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.

Computerized systems – All the components necessary to capture, process, transfer, store, display and manage information, including (but not limited to) hardware, software, personnel and documentation.

Drug establishment licence – A licence issued to a person in Canada to conduct licensable activities in a building which has been inspected and assessed as being in compliance with the requirements of Divisions 2 to 4 of the Food and Drug Regulations.

IT Infrastructure – The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Life cycle – All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

Process owner – The person responsible for the business process.

System owner – The person responsible for the availability, and maintenance of a computerized system and for the security of the data residing on that system.

Third Party – Parties not directly managed by an establishment licence holder.

Appendix B – References

Legislation

Canadian Acts and regulations can be found on the Justice Canada website
http://www.justice.gc.ca

Food and Drugs Act
http://laws-lois.justice.gc.ca/eng/acts/F-27/index.html

Food and Drug Regulations
http://laws-lois.justice.gc.ca/eng/regulations/C.R.C.,_c._870/index.html

Health Canada Guidance

Good manufacturing practices guide for drug products (GUI-0001):
https://www.canada.ca/en/health-canada/services/drugs-health-products/compliance-enforcement/good-manufacturing-practices/guidance-documents/gmp-guidelines-0001.html

Guide to validation – drugs and supporting activities (GUI-0029):
https://www.canada.ca/en/health-canada/services/drugs-health-products/compliance-enforcement/good-manufacturing-practices/validation/validation-guidelines-pharmaceutical-dosage-forms-0029.html

International Guidance

ASTM E2500 - 13 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment:
www.astm.org/Standards/E2500.htm

Pharmaceutical Inspection Cooperation Scheme's (PIC/S) - Annex 11 Computerized Systems (PE 009-15):
https://www.picscheme.org/en/publications?tri=gmp

Pharmaceutical Inspection Cooperation Scheme's (PIC/S) - Good Practices for Computerised Systems in Regulated "GXP" Environments (PI 011-3):
https://www.picscheme.org/en/publications?tri=all

The Institute of Electrical and Electronics Engineers Standards Association (IEEE SA):
https://standards.ieee.org/

The International Organization for Standardization (ISO):
https://www.iso.org/standards.html