World Health Organization

# GUIDELINES ON VALIDATION – APPENDIX 5 VALIDATION OF COMPUTERIZED SYSTEMS

**(May 2018)**

***DRAFT FOR COMMENTS***

Should you have any comments on the attached text, please send these to Dr S. Kopp, Group Lead, Medicines Quality Assurance, Technologies Standards and Norms (kopps@who.int) with a copy to Ms Xenia Finnerty (finnertyk@who.int) by **20 June 2018**.

**Medicines Quality Assurance working documents will be sent out electronically only and will also be placed on the Medicines website for comment under "Current projects". If you do not already receive our draft working documents please let us have your email address and we will add it to our electronic mailing list.**

This draft is intended for a restricted audience only, i.e. the individuals and organizations having received this draft. The draft may not be reviewed, abstracted, quoted, reproduced, transmitted, distributed, translated or adapted, in part or in whole, in any form or by any means outside these individuals and organizations (including the organizations' concerned staff and member organizations) without the permission of the World Health Organization. The draft should not be displayed on any website.

Please send any request for permission to:

Dr Sabine Kopp, Group Lead, Medicines Quality Assurance, Technologies Standards and Norms, Regulation of Medicines and other Health Technologies, Department of Essential Medicines and Health Products, World Health Organization, CH-1211 Geneva 27, Switzerland. Fax: (41-22) 791 4730; email: kopps@who.int.

The designations employed and the presentation of the material in this draft do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the World Health Organization in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by the World Health Organization to verify the information contained in this draft. However, the printed material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the World Health Organization be liable for damages arising from its use.

This draft does not necessarily represent the decisions or the stated policy of the World Health Organization.

SCHEDULE FOR THE PROPOSED ADOPTION PROCESS OF DOCUMENT QAS/16.667:

## GUIDELINES ON VALIDATION – APPENDIX 5
## VALIDATION OF COMPUTERIZED SYSTEMS

| | |
|---|---|
| Discussion of proposed need for revision in view of the current trends in validation during informal consultation on data management, bioequivalence, GMP and medicines' inspection | 29 June–<br>1 July 2015 |
| Preparation of draft proposal for revision of the main text and several appendices by specialists in collaboration with the Medicines Quality Assurance Group and Prequalification Team (PQT)-Inspections, based on the feedback received during the meeting and from PQT-Inspections, draft proposals developed on the various topics by specialists, as identified in the individual working documents. | July 2015–<br>April 2016 |
| Presentation of the progress made to the fiftieth meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations | 12–16 October 2015 |
| Discussion at the informal consultation on good practices for health products manufacture and inspection, Geneva | 4–6 April 2016 |
| Preparation of revised text by Mrs M. Cahilly and Dr A.J. van Zyl, participants at the above-mentioned consultation, based on Mrs Cahilly's initial proposal and the feedback received during and after the informal consultation by the meeting participants and members of PQT-Inspections | May 2016 |
| Circulation of revised working document for public consultation | May 2016 |
| Consolidation of comments received and review of feedback | August–September 2016 |
| Presentation to the fifty-first meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations | 17–21 October 2016 |
| More than 400 comments were received during the public consultation and were evaluated and prioritized by the German Expert Group on Computerized System with the kind assistance of Mr Menges | October 2016–April 2017 |
| The comments and feedback were discussed and further reviewed during the consultation on Good practices for health products manufacturer and inspection | 25–28 April 2017 |
| The large number of feedback and comments received needed a major restructuring and reworking, assistance was sought from experts and PQT-Inspections | May 2017–<br>December 2017 |

| | |
|---|---|
| Preparation of revised text by Dr Dimitrios Catsoulacos form the PQT-Inspection and Dr Valeria Gigante from the Medicine Quality Assurance Group based on the comments and all the various input received | February–April 2018 |
| Circulation of revised working document for public consultation | June 2018 |
| Consolidation of comments received during the public consultation | July 2018 |
| Presentation of the revised working document to the WHO consultation on Good practices for health products manufacture and inspection | 10–12 July 2018 |
| Revision of the draft text on the basis of feedback received during and after the informal consultation by the meeting participants and members of PQT-Inspections | July 2018 |
| Circulation of revised working document for public consultation | July–September 2018 |
| Compilation of comments received during the public consultation | October 2018 |
| Presentation of updated working document to fifty-third meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations | 22–26 October 2018 |
| Any other follow-up action as required | … |

# VALIDATION OF COMPUTERIZED SYSTEMS

## Contents

## 1. BACKGROUND INFORMATION

The need for revision of the published World Health Organization (WHO) *Supplementary guidelines on good manufacturing practices: validation (1)* was identified by the Prequalification of Medicines Programme and a first draft document was circulated for comment in early 2013. The focus at that time was the revision of the *Appendix on non-sterile process validation* (Appendix 7), which had been revised and was adopted by the Committee at its forty-ninth meeting in October 2014 *(2)*.

The overarching text, entitled *"Guidelines on Validation*" (working document QAS/16.666) constitutes the general principles of the new guidance on validation. This working document, the ***Validation of computerized systems,*** is the Appendix 5 of the overarching guidances on validation.

The following is an overview of the appendices that are intended to complement the general text on validation:

*Appendix 1*
*Validation of heating, ventilation and air-conditioning systems*
→ will be replaced by cross-reference to WHO good manufacturing practices for heating, ventilation and air-conditioning systems for non-sterile pharmaceutical products.

*Appendix 2*
*Validation of water systems for pharmaceutical use*
→ will be replaced by cross-reference to WHO good manufacturing practices: water for pharmaceutical use *(3)*.

*Appendix 3*
*Cleaning validation* – consensus to retain

*Appendix 4*
*Analytical method validation – update in process* (working document QAS/16.671)

***Appendix 5***
***Validation of computerized systems* – updated text proposed in this working document**

*Appendix 6*
*Qualification of systems and equipment – update in process* (working document QAS/16.673/Rev.1)

*Appendix 7*
*Non-sterile process validation – update already published as Annex 3, WHO Technical Report Series, No. 992, 2015.*

## 2. INTRODUCTION AND SCOPE

2.1 Computerized systems should be validated in accordance with quality risk management principles and the level of validation should be commensurate to identified risks, complexity and intended use. This guide applies to systems used in good manufacturing practices (GMP) *(4)* but may be extended to systems used in all good practice (GXP) activities, as appropriate.

2.2 The purpose of validation is to confirm that the computerized system specifications conform to the user's needs and intended use by examination and provision of documented and objective evidence that the particular requirements can be consistently fulfilled. Validation should establish confidence in the accuracy, reliability and consistency in performance of the system and it should also ensure that all necessary technical and procedural controls are implemented confirming compliance with good documentation practices for electronic data generated by the system *(5).*

2.3 System elements that need to be considered in computerized system validation include computer hardware and software, related equipment and network components and operating system environment, procedures and systems documentation, as appropriate, including user manuals. Persons should be appropriately trained and qualified, and including but not limited to, end users, system application administrators, network engineers, database administrators and electronic archivers. Computerized system validation activities should address both system functionality and configuration as well as any custom-developed elements.

2.4 Computerized systems should be maintained in a validated state with risk-based controls for the operational phase which may include but is not limited to system planning, preparation and verification of standard operating procedures (SOPs) and training programs, system operation and maintenance including handling of software and hardware updates, monitoring and review, change management and incident reporting followed by system retirement.

2.5 Depending on the types of systems or typical applications such as process control systems (distributed control system (DCS), programable logic controller (PLC), supervisory control and data acquisition (SCADA)), laboratory information management systems (LIMS), laboratory instrument control systems and business systems (enterprise resource planning (ERP), manufacturing resource planning (MRP II)) used by the manufacturer, documentation covering, but not limited to, the following information should be accessible on-site:

- purpose and scope;
- roles and responsibilities;
- validation approach;
- risk management principles;

- system acceptance criteria;
- vendor selection and assessment;
- computerized system validation steps;
- configuration management and change control procedures;
- back-up and recovery;
- error handling and corrective action;
- contingency planning and disaster recovery;
- maintenance and support;
- system requirement;
- validation deliverables and documentation;
- template, formats, annex;
- examples.

## 3. GLOSSARY

The definitions given below apply to the terms used in these guidelines. They may have different meanings in other contexts.

**archival.** Archiving is the process of protecting records from the possibility of being further altered or deleted, and storing these records under the control of independent data management personnel throughout the required retention period. Archived records should include, for example, associated metadata and electronic signatures.

**audit trail.** The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the "who, what, when and why" of the action.

For example, in a paper record, an audit trail of a change would be documented via a single-line cross-out that allows the original entry to remain legible and documents the initials of the person making the change, the date of the change and the reason for the change, as required to substantiate and justify the change. In electronic records, secure, computer-generated, time-stamped audit trails should allow for reconstruction of the course of events relating to the creation, modification and deletion of electronic data. Computer-generated audit trails should retain the original entry and document the user identification, the time/date stamp of the action, as well as the reason for the change, as required to substantiate and justify the action. Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system, specific electronic records or specific data contained within the record.

**automatic or live update.** It is used to bring up to date software and system functionalities in a silent or announced way. More specifically the update takes place automatically with or without the user's knowledge.

**backup.** A backup means a copy of one or more electronic files created as an alternative in case the original data or system are lost or become unusable (for example, in the event of a system crash or corruption of a disk). It is important to note that backup differs from archival in that back-up copies of electronic records are typically only temporarily stored for the purposes of disaster recovery and may be periodically overwritten. Such temporary back-up copies should not be relied upon as an archival mechanism.

**business continuity plan.** A documented plan that defines the ongoing process supported by management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans and assure continuity of services through personnel training, plan testing and maintenance.

**cloud based.** A model for enabling on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. These computing resources should be appropriately qualified.

**computerized system.** A computerized system collectively controls the performance and execution of one or more automated processes and/or functions. It includes computer hardware, software, peripheral devices, networks and documentation, e.g. manuals and standard operating procedures, as well as  personnel interacting with  hardware and software.

**computerized systems validation.** Confirmation by examination and provision of objective and documented evidence that computerized system’s predetermined specifications conform to user needs and intended use and that all requirements can be consistently fulfilled.

**configuration management.** A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status and verifying compliance with specified requirements.

**COTS.** Commercial off-the-shelf software; a vendor-supplied software component of a computerized system for which the user cannot claim complete software life-cycle control.

**data.** All original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, which are generated or recorded at the time of the good manufacturing practices (GMP) activity and allow full and complete reconstruction and evaluation of the GMP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GMP activities is recorded.

**data integrity**. Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, such that they are attributable, legible, contemporaneously recorded, original or a true copy and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices *(5).*

**data life cycle.** All phases of the process by which data are created, recorded, processed, reviewed, analyzed and reported, transferred, stored and retrieved and monitored until retirement and disposal. There should be a planned approach to assessing, monitoring and managing the data and the risks to those data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle.

**disaster recovery.** It is a documented process or set of procedures to recover and protect a business information technology infrastructure in the event of a disaster. It appropriately defines resources and actions to be taken before, during and after a disaster.

**functional specifications.** The functional specifications document, if created, defines functions and technological solutions that are specified for the computerized system based upon technical requirements needed to satisfy user requirements (e.g. specified bandwidth required to meet the user requirement for anticipated system usage).

**legacy system**. It refers to outdated computer system, programming language, application software, or process that are used instead of available upgraded versions and are deemed not to fully satisfy current good manufacturing practices requirements.

**master data.** It is a single source of business data used across multiple systems, applications, and processes and subject to change control to ensure accuracy through the data life cycle.

**metadata.** Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. Metadata necessary to evaluate the meaning of data should be securely linked to the data and subject to adequate review. For example, in weighing, the number 8 is meaningless without metadata, i.e. the unit, mg. Other examples of metadata include the time/date stamp of an activity, the operator identification (ID) of the person who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.

**production environment.** For regulated computerized systems, the production environment is the business and computing operating environment in which the computerized system is being used for good manufacturing practices regulated purposes.

**regression analysis and testing.** A documented software verification and validation task to determine the extent of verification and validation analysis and testing that must be repeated when changes are made to any previously examined software component or system.

**system life cycle.** The period of time that starts when a computerized system is conceived and ends when the system is retired taking into consideration regulatory requirements. The system life cycle typically includes a requirements and planning phase; a development phase that includes: a design phase and a programming and testing phase; a qualification and release phase that includes: system integration and testing phase; validation phase; release phase; an operation and maintenance phase; and finally a system retirement phase.

**user acceptance testing.** Verification of the fully-configured computerized system installed in the production environment (or in a test environment equivalent to the production environment) to perform as intended in the business process when operated by end-users trained in end-user standard operating procedures that define system use and control. User-acceptance testing may be a component of the performance qualification (PQ) or a validation step separate from the PQ.

**user requirements specification.** The user requirements specification, if prepared as a separate document, is a formal document that defines the requirements for use of the computerized system in its intended production environment.

## 4. COMPUTERIZED SYSTEM VALIDATION PROTOCOLS AND REPORTS

4.1 A computerized system needs to be validated according to an approved protocol and final report including results and conclusions prior to routine use.

### Validation protocol

4.2 Validation should be executed in accordance with the validation protocol and applicable written procedures.

4.3 A validation protocol should define the objectives, the validation strategy, including roles and responsibilities and documentation and activities to be performed. The protocol should at least cover the scope, risk management approach, the specification, testing, review and release of the computerized system for GMP use.

4.4 The validation protocol should be tailored to the system type, impact, risks and requirements applicable to the system for which it governs validation activities.

### Validation report

4.5 A validation report should be prepared, summarizing system validation activities.

4.6 It should make reference to the protocol and outline the validation process, and include an evaluation and conclusion on results. Deviations from the validation protocol and applicable written procedures should be described, investigated, assessed and justification for their acceptance or rejection should be documented.

4.7 Results should be recorded, reviewed, analyzed and compared against the predetermined acceptance criteria. All critical and major test discrepancies that occurred during the verification/validation testing, should be investigated and if accepted they should be appropriately justified.

4.8 The conclusion of the report should state whether or not the outcome of the validation was considered successful and should make recommendations for future monitoring where applicable. The report should be approved after appropriately addressing any issue identified during validation and the system should then be released for GMP use.

## 5. VENDOR MANAGEMENT

5.1 When third parties (e.g. vendors, service providers) are used, e.g. to provide, install, configure, validate, maintain, modify or retain a computerized system or related service or for data processing or system components, including cloud-based systems, an evaluation of the vendor-supplied system or service and the vendor’s quality systems should be conducted and recorded. The scope and depth of this evaluation should be based upon risk management principles.

5.2 The competence and reliability of a vendor are key factors when selecting a product and/or service provider and vendor management is an on-going process that requires periodic assessment and review. Vendor evaluation activities may include but are not limited to: completion of a quality related questionnaire by the vendor; gathering of vendor documentation related to system development, testing and maintenance including vendor procedures, specifications, system architecture diagrams, test evidence, release notes and other relevant vendor documentation; an on-site audit of the vendor's facilities should be conducted to evaluate the vendor's system life-cycle control procedures, practices and documentation.

5.3 A contract should be in place between the manufacturer and the vendor and/or the service provider defining the roles and responsibilities and quality procedures for both parties, throughout the system life cycle. The contract acceptor should not pass to a third party any of the work entrusted to her/him under the contract without the manufacturer's prior evaluation and approval of the arrangements.

## 5. REQUIREMENTS SPECIFICATIONS

6.1 Requirements specifications should be written to document user requirements and functional or operational requirements and performance requirements. Requirements may be documented in separate user requirements specifications (URS) and functional requirements specifications (FRS) documents or in a combined document.

### User requirements specifications

6.2 The authorized URS document, or equivalent, should describe the intended uses of the proposed computerized system and should define critical data and data life-cycle controls that will assure consistent and reliable data throughout the processes by which data is created, processed, transmitted, reviewed, reported, retained and retrieved and eventually disposed.

6.3 The URS should be written in a way to ensure that the data will meet regulatory requirements such as the *WHO Guidance on good data and record management practices (5).*

6.4 Other aspects that should be specified include, but are not limited to, those related to:

- the data to be entered, processed, reported, stored and retrieved by the system, including any master data and other data considered to be the most critical to system control and data output;
- the flow of data including that of the business process(es) in which the system will be

used as well as the physical transfer of the data from the system to other systems or network components. Documentation of data flows and data process maps are recommended to facilitate the assessment and mitigation and control of data integrity risks across the actual, intended data process(es);

- networks and operating system environments that support the data flows;
- how the system interfaces with other systems;
- the operating program;
- synchronization and security controls of time/date stamps;
- controls of both the application software as well as operating systems to assure system access only to authorized persons;
- controls to ensure that data will be attributable to unique individuals (for example, to prohibit use of shared or generic login credentials);
- controls to ensure that data is legibly and contemporaneously recorded to durable ("permanent") media at the time of each step and event and controls that enforce the sequencing of each step and event (for example, controls that prevent alteration of data in temporary memory in a manner that would not be documented);
- controls that assure that all steps that create, modify or delete electronic data will be recorded in independent, computer-generated audit trails or other metadata or alternate documents that record the "what" (e.g. original entry), "who" (e.g. user identification), "when" (e.g. time/date stamp) and "why" (e.g. reason) of the action;
- backups and the ability to restore the system and data from backups;
- the ability to archive and retrieve the electronic data in a manner that assures that the archive copy preserves the full content of the original electronic data set, including all metadata needed to fully reconstruct the GMP activity. The archive copy should also preserve the meaning of the original electronic data set;
- input/output checks, including implementation of procedures for the review of original electronic data and metadata, such as audit trails;
- controls for electronic signatures;
- alarms and flags that indicate alarm conditions and invalid and altered data in order to facilitate detection and review of these events;
- system documentation, including system specifications documents, user manuals and procedures for system use, data review and system administration;
- system capacity and volume requirements based upon the predicted system usage and performance requirements;
- performance monitoring of the system;
- controls for orderly system shutdown and recovery;
- business continuity.

6.5 The extent and detail of the requirements should be commensurate with the operational risk and the complexity of the computerized system. User requirements should be specific and be phrased in a way to support their testing or verification within the computerized system's context.

**Functional specifications**

6.6 Functional specifications should describe in detail the functions, performances and interfaces of the computerized system based upon technical requirements needed to satisfy user requirements.

6.7 The functional specifications provide a basis for the system design and configuration specifications. Functional specifications should consider requirements for operation of the computerized system in the intended computing environment, such as functions provided by vendor-supplied software as well as functions required for user business processes that are not met by commercial off-the-shelf software (COTS) functionality and default configurations that will require custom code development. Network infrastructure requirements should also be taken into account. Each described function should be verifiable.

6.8 Personnel access roles that provide the ability and/or authorization to write, alter or access programs should be defined and qualified. There should be appropriate segregation of roles between personnel responsible for the business process and personnel for system administration and maintenance.

## 7. SYSTEM DESIGN AND CONFIGURATION SPECIFICATIONS

7.1 System design and configuration specifications should be developed based on user and functional requirements. Specification of design parameters and configuration settings (separate or combined) should ensure data integrity and compliance with the *WHO guidance on good data and record management practices (5).*

7.2 System design and configuration specifications should provide a high-level system description as well as an overview of the system physical and logical architecture and should map out the system business process and relevant work flows and data flows if these have not already been documented in other requirements specifications documents.

7.3 The system design and configuration specifications may include, as applicable, a software design specification in case of code development and configuration specifications of the software application parameters, such as security profiles, audit trail configuration, data libraries and other configurable elements.

7.4 In addition, the system design and configuration specifications may also include, based upon risk, the hardware design and its configuration specifications as well as that of any supporting network infrastructure.

7.5 System design and configuration specifications should include secure, protected, independent computer-generated audit trails to track configuration changes to critical  settings in the system.

## 8. DESIGN QUALIFICATION

8.1 A design review should be conducted to verify that the proposed design and configuration of the system is suitable for its intended purpose and will meet all applicable user and functional requirements specifications.

8.2 It may include a review of vendor documentation, if applicable, and verification that requirements specifications are traceable to proposed design and configuration specifications.

## 9. BUILD AND PROJECT IMPLEMENTATION

9.1 Once the system requirements and the system design and configuration are specified and verified, where applicable, system development activities may begin. The development activities may occur as a dedicated phase following completion of specification of system requirements, design and configuration. Alternatively, development activities may occur iteratively as requirements are specified and verified (such as when prototyping or rapid-development methodologies are employed).

### Vendor-supplied systems

9.2 For vendor-supplied systems, development controls for the vendor-supplied portion of the computerized system should be assessed during the vendor evaluation or supplier qualification. For vendor-supplied systems that include custom components (such as custom-coded interfaces or custom report tools) and/or require configuration (such as configuration of security profiles in the software or configuration of the hardware within the network infrastructure), the system should be developed under an appropriate documented quality management system.

### Custom-developed systems

9.3 For custom-developed systems and configurable systems, the system should be developed under an appropriate documented quality system. For these systems or modules the quality management system controls should include development of code in accordance with documented programing standards, review of code for adherence to programing standards and design specifications and development testing that may include unit testing and module/integration testing.

9.4 System prototyping and rapid, agile development methodologies may be employed during the system build and development testing phase. There should be an adequate level of documentation of these activities.

**Preparation for the system qualification phases**

9.5 The system development and build phase should be followed by the system qualification phase. This typically consists of installation, operational and performance testing. Actual qualification required may vary depending on the scope of the validation project as defined in the validation plan and based upon a documented and justified risk assessment.

9.6 Prior to the initiation of the system qualification phase, the software program and requirements and specifications documents should be finalized and subsequently managed under formal change control.

9.7 Persons who will be conducting the system qualification should be trained to adhere to the following requirements for system qualification:

- test documentation should be generated to provide evidence of testing;
- test documentation should comply with good documentation practices;
- any discrepancies between actual test results and expected results should be documented and adequately resolved based upon risk prior to proceeding to subsequent test phases.

## 10. INSTALLATION QUALIFICATION

10.1 Installation qualification (IQ), also referred to as installation verification testing should provide documented evidence that the computerized system, including software and associated hardware, is installed and configured in the intended system test and production environments according to written specifications.

10.2 The IQ will verify, for example, that the computer hardware on which the software application is installed has the proper firmware and operating system, that all components are present and in the proper condition and that each component is installed per the manufacturer or developer instructions.

10.3 IQ should include verification that configurable elements of the system are appropriately set as specified. Where appropriate, this could also be done during operational qualification (OQ).

## 11. OPERATIONAL QUALIFICATION

11.1 The OQ, or operational/functional verification testing, should provide documented evidence that software and hardware function as intended over anticipated operating ranges.

11.2 Functional testing should include, based upon risk:

- an appropriate degree of challenge testing (such as boundary, range, limit, nonsense entry testing) to verify the system appropriately handles erroneous entries or erroneous use;
- verification that alarms are raised based upon alarm conditions;
- flags are raised to signal invalid or altered data.

## 12. STANDARD OPERATING PROCEDURES AND TRAINING

12.1 Prior to the conduct of the performance qualification (PQ) and user acceptance testing (UAT), and prior to the release of the computerized system, there should be adequate written procedures and documents and training programmes created defining system use and control. These may include vendor-supplied user manuals as well as SOPs and training programs developed in-house.

12.2 Procedures and training programs that should be developed include, but are not necessarily limited to:

- system use procedures that address:
  - routine operation and use of the system in the intended business process(es),
  - review of the electronic data and associated metadata (such as audit trails) and how the source electronic records will be reconciled with printouts, if any,
  - mechanisms for signing electronic data,
  - system training requirements prior to being granted system access;

- system administration procedures that address:
  - granting and disabling user access and maintaining security controls,
  - backup/restore,
  - archival/retrieval,
  - disaster recovery and business continuity,
  - change management,

- incident and problem management,
- system maintenance.

## 13. PERFORMANCE QUALIFICATION AND USER ACCEPTANCE TESTING

13.1 PQ, that includes UAT, should be conducted to verify the intended system use and administration defined in the URS and design qualification (DQ), or equivalent document.

13.2 The PQ should be conducted in the live environment or in a test environment that is equivalent to the live environment in terms of overall software and hardware configuration.

13.3 PQ testing should also include, as applicable, an appropriate degree of stress/load/volume testing based upon the anticipated system use and performance requirements in the production environment.

13.4 In addition, an appropriate degree of end-to-end or regression testing of the system should be conducted to verify the system performs reliably when system components are integrated in the fully-configured system deployed in the production environment.

13.5 UAT should be conducted by system users to verify the adequacy of system, use of SOPs and training programs. The UAT should include verification of the ability to generate and process only valid data within the computerized system, including the ability to efficiently review electronic data and metadata, such as audit trails.

### Legacy systems

13.6 The continued use of a legacy system should be justified by demonstrating the system continues to be relevant to the GMP process being supported and by ensuring adequate validation of the system has been performed.

13.7 The validation approach to be taken should aim at providing data and information to support the retrospective documentation of the system as well as requalification evidence.

13.8 A risk assessment should be undertaken to determine the criticality of the system to the process or operation being supported and a gap analysis should identify the level of completeness of existing qualification documentation (e.g. URS, IQ/OQ/PQ, SOPs) and state of system control, operation and maintenance.

13.9 For legacy systems, because of their age and unique characteristics, the system development documentation and records appropriate for validation may not be available. Nevertheless, the strategy should be consistent with validation principles where assurance is established, based on compilation and formal review of the history of use, maintenance, error report and change control system records. These activities should be based on documented URS. If historical data do not encompass the current range of operating parameters, or if there have been significant changes between past and current practices, then retrospective data would not of itself support validation of the current system.

13.10 The validation exercise should demonstrate that user requirements and system description have been appropriately established as well as provide evidence that the system has been qualified and accepted and that GXP requirements are met.

13.11 System retirement should be considered as a system life-cycle phase. It should be planned, risk-based and documented. If migration or archiving of GMP-relevant data *(4)* is necessary, the process must be documented.

13.12 Where electronic data are transferred from one system to another it should be demonstrated that data are not altered during the migration process. Conversion of data to a different format should be considered as data migration. Where data are transferred to another medium, data must be verified as an exact copy prior to any destruction of the original data.

13.13 Data migration efforts may vary greatly in complexity and measures to ensure appropriate transfer of data should be commensurate to identified risks. Migrated data should remain usable and should retain its content and meaning. The value and/or meaning of and links between a system audit trail and electronic signatures should be ensured in a migration process.

## 14. SYSTEM OPERATION AND MAINTENANCE

### Security and access control

14.1 Manufacturers should have systems and procedures in place to ensure security of data integrity and access control to computerized systems.

14.2 Suitable security measures should be in place to prevent unauthorized entry or manipulation or deletion of data through both the application software as well as in operating system environments in which data may be stored or transmitted. Data should be entered or amended only by persons authorized to do so.

14.3 The activity of entering data, changing or amending incorrect entries and creating backups should be done in accordance with SOPs.

14.4 Security should extend to devices used to store programs. Access to these devices should be controlled.

14.5 Procedures for review of audit trails and when necessary metadata should define the frequency, roles and responsibilities, and nature of these reviews.

14.6 Actions, performance of the system and acquisition of data should be traceable and identify the persons who made entries and or changes, approved decisions or performed other critical steps in system use or control.

14.7 Details on user profiles, access rights to systems, networks, servers, computerized systems and software should be documented and an up-to-date list on the individual user rights for the software, individual computer systems and networks should be maintained and subjected to change control. The level of detail should be sufficient to enable computer system validation personnel, information technology (IT) personnel/any external auditor/inspector to ascertain that security features of the system and of software used to obtain and process critical data cannot be circumvented.

14.8 All GMP computerized systems, either stand-alone or in a network, should have a system commensurate to identified risks for monitoring through an audit trail events that are relevant. These events should include all elements that need to be monitored to ensure that the integrity *(5)* of the data could not have been compromised, such as but not limited to, changes in data, deletion of data, dates, times, backups, archives, changes in user access rights, addition/deletion of users and logins. In accordance with *WHO guidance on good data and record management practices (5).* The configuration and archival of these audit trails should be documented and also be subjected to change control. These audit trails should be accurate, consistent, secure and available throughout the retention period and their generation appropriately qualified.

**Operation and maintenance**

14.9 Entry of  data into a computerized system should be verified by an independent authorized person and locked before release for routine use.

14.10 Validated computerized systems should be maintained in a validated state once released to the GXP production environment.

14.11 There should be written procedures governing system operation and maintenance, including, for example:

- performance monitoring;
- change management and configuration management;
- problem/incident management;
- program and data security;
- program and data backup/restore and archival/retrieval;
- system administration and maintenance;
- data flow and data life cycle;
- system use and review of electronic data and metadata (such as audit trails);
- personnel training;
- disaster recovery and business continuity;
- availability of spare parts and technical support;
- periodic re-evaluation.

### Periodic review

14.12 Computerized systems should be periodically reviewed to determine whether the system remains in a validated state or whether there is a need for revalidation. The scope and extent of the revalidation should be determined using a risk-based approach. The review should at least cover:

- review of changes;
- review of deviations;
- review of incidents/ events;
- systems documentation;
- procedures;
- training;
- effectiveness of corrective and preventive action (CAPA).

14.13 CAPA should be taken where indicated as a result of the periodic review.

14.14 Automatic or live updates should be subject to review prior to becoming effective.

## 15. SYSTEM RETIREMENT

15.1 Once the computerized system or components are no longer needed, the system or components should be retired and decommissioned in accordance with established authorized procedures including a change control procedure and a formal plan for retirement.

15.2 Records should be in a readable form and in a manner that preserves the content and meaning of the source electronic records throughout the required records retention period.

15.3 The outcome of the retirement activities, including traceability of the data and computerized systems, should be presented in a report.

## 16. REFERENCES

1. Supplementary guidelines on good manufacturing practices: *validation*. WHO Technical Report Series, No. 937, 2006, Annex 4.

2. Supplementary guidelines on good manufacturing practice: validation. Qualification of systems and equipment. WHO Technical Report Series, No. 937, 2006, Annex 4, Appendix 7 (update in progress QAS/16.673/Rev.1).

3. WHO good manufacturing practices: water for pharmaceutical use. WHO Technical Report Series No. 970, 2012, Annex 2.

4. WHO good manufacturing practices for pharmaceutical products: main principles. WHO Technical Report Series, No. 986, 2014, Annex 2.

5. Guidance on good data and record management practices. WHO Technical Report Series, No. 996, 2016, Annex 5.

**Further reading**

OECD series on principles of Good laboratory practice and compliance monitoring Number 17. Advisory document of the working group on Good Laboratory Practice application of GLP principles to computerised systems, 2016.

Computerised systems. In: The rules governing medicinal products in the European Union. Volume 4: Good manufacturing practice (GMP) guidelines: Annex 11. Brussels: European Commission (http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-4/pdfs-en/anx11en.pdf).

Drug Information Association. Computerized Systems Used in Nonclinical Safety Assessment; Current Concepts in Validation and Compliance. Horsham, PA: Drug Information Association (DIA), 2008.

GAMP® 5 – A Risk-Based Approach to Compliant GxP Computerized Systems. Tampa, FL: GAMP Forum, International Society for Pharmaceutical Engineering (ISPE); 2008.

GAMP® good practice guide: A risk-based approach to GxP compliant laboratory computerized systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2012.

GAMP® Good Practice Guide: A Risk-Based Approach to GxP Process Control Systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2011.

GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems – A Companion Volume to GAMP®5. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2010.

GAMP® Good Practice Guide: A Risk-Based Approach to Regulated Mobile Applications. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2014.

GAMP® Good Practice Guide: A Risk-Based Approach to Testing of GxP Systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2012.

GAMP® Good Practice Guide: Global Information Systems Control and Compliance. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2005.

GAMP® Good Practice Guide: IT Infrastructure Control and Compliance. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2005.

GAMP® Good Practice Guide: Manufacturing Execution Systems – A Strategic and Program Management Approach. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2010.

National Institute of Standards and Technology, U.S. Department of Commerce, (NIST) Cloud Computing References: http://www.nist.gov/itl/cloud/index.cfm.

Official Medicines Control Laboratories Network of the Council of Europe: Quality assurance documents: PA/PH/OMCL (08) 69 3R – Validation of computerised systems – core document (https://www.edqm.eu/sites/default/files/medias/fichiers/Validation_of_Computerised_Systems_Core_Document.pdf) and its annexes:

- PA/PH/OMCL (08) 87 2R – Annex 1: Validation of computerised calculation systems: example of validation of in-house software
- (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_1_Validation_of_computerised_calculation.pdf).
- PA/PH/OMCL (08) 88 R – Annex 2: Validation of databases (DB), laboratory

information management systems (LIMS) and electronic laboratory notebooks (ELN)

- (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_2_Validation_of_Databases_DB_Laboratory_.pdf).

- PA/PH/OMCL (08) 89 R – Annex 3: Validation of computers as part of test equipment (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_3_Validation_of_computers_as_part_of_tes.pdf).

- PA/PH/OMCL (08) 69 R7 - Annex 17: Application of GLP Principles to Computerised Systems. (http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/jm/mono(2016)13&doclanguage=en).

Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic records; electronic signatures. US Food and Drug Administration. The current status of 21 CFR Part 11 Guidance is located under Regulations and Guidance at: http://www.fda.gov/cder/gmp/index.htm — see background: http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf.

PIC/S guide to good manufacturing practice for medicinal products annexes: Annex 11 – Computerised systems. Geneva: Pharmaceutical Inspection Co-operation Scheme.

PIC/S PI 011-3 Good practices for computerised systems in regulated GxP environments. Geneva: Pharmaceutical Inspection Co-operation Scheme

***