OMCL Network of the Council of Europe QUALITY ASSURANCE DOCUMENT

PA/PH/OMCL (08) 69 3R

VALIDATION OF COMPUTERISED SYSTEMS

CORE DOCUMENT

Full document title and reference	Validation of Computerised Systems - Core Document PA/PH/OMCL (08) 69 3R
Document type	Guideline
Legislative basis	-
Date of first adoption	May 2009
Date of original entry into force	July 2009
Date of entry into force of revised document	-
Previous titles/other references	-
Custodian Organisation	The present document was elaborated by the OMCL Network/EDQM of the Council of Europe
Concerned Network	GEON

VALIDATION OF COMPUTERISED SYSTEMS
CORE DOCUMENT

SCOPE

This guideline defines basic principles for the validation of computerised systems used within Official Medicines Control Laboratories (OMCLs) with impact on quality of results. The purpose of this validation is to guarantee the confidence in scientific results obtained with each computerised system. A validated system ensures accurate results and reduces the risk of failure of the system.

This document covers in-house and commercial software for calculation, database computerised systems, Laboratory Information Management Systems (LIMS), Electronic Laboratory Notebooks (ELN) and computers as part of test equipment.

INTRODUCTION

This guideline outlines general validation principles for computerised systems of OMCLs in accordance with ISO/IEC 17025. It gives general requirements and it also lists the minimum elements required for the validation of different types of software. Actually, due to the great variety of software, it is not possible to state in one single document all the specific validation elements that are applicable.

This guideline is intended for use by OMCLs working under Quality Management Systems based on the ISO/IEC 17025 standard, which use computerised systems for a part or the totality of the processes related to the quality control of medicines, and it is not addressed to manufacturers working under GMP requirements.

In order to simplify the management of the guideline, the present document contains only a general introduction and general requirements for different types of computerised systems. The core document is supplemented with system-related annexes, containing additional requirements and/or practical examples of validation documentation, which are to be used in combination with the general recommendations given in the core document.

The list of annexes, included in this document, will be updated as soon as new annexes are issued.

This document should be considered as a guide to OMCLs for planning, performing and documenting the validation of their computerised systems. It should not be taken as a list of compulsory requirements. It is left to the professional judgement and background experience of each OMCL to decide on the most relevant procedures to be undertaken in order to give evidence that their computerised systems are working properly and are appropriate for their intended use.

DEFINITIONS

Computer system: Computer hardware components assembled to perform in conjunction with a set of software programmes, which are collectively designed to perform a specific function or group of functions.

Computerised system: a computer system plus the controlled function that it operates. Includes hardware, software, peripheral devices, personnel, and documentation; e.g., manuals and Standard Operating Procedures (SOPs).

Commercial (off-the-shelf, configurable) software: Configurable programmes that can be configured to specific user applications by "filling in the blanks", without altering the basic programme.

In-house developed software: system developed by the user (or by a contracted company), with the purpose of specifically meeting a defined set of user requirements.

Electronic laboratory notebook (ELN): software programme designed to replace paper laboratory notebooks.

Laboratory Information Management System (LIMS): Automated laboratory systems that collect and manage data.

1. HARDWARE

The hardware used shall fulfil the technical requirements so that the work to be completed can be carried out. Such requirements include e.g. minimum system requirements indicated by the manufacturer of the equipment. These requirements should be predefined in accordance with the intended use.

The hardware components shall be installed by skilled personnel (e.g. staff from the Information Technology (IT) Unit, the technician from the manufacturer of the equipment, or other trained personnel), and shall be checked for their functionality and compared with the requirements.

Computerised systems that are part of test equipment must be labelled unambiguously.

For computerised systems which are components of test equipment, records must be kept on hardware configuration, installation and changes. These records can be entered in the logbook of the test equipment.

2. GENERAL REQUIREMENTS FOR SOFTWARE

Inventory

An inventory or listing of all computerised systems should be available.

The following minimum information should be included in the computerised systems inventory:

- unique identification
- purpose
- validation status
- physical or storage (drive and files path) location of the software and related documentation
- responsible or contact person

In the case of local installation (workstation), each copy of the software needs its own unique identification.

In the case of software related to scientific equipment (e.g. HPLC) its identification (such as licence number or serial number, and version number) should be independent from the equipment identification, whenever possible.

Validation of the software

Prior to routine use, the software should be validated.

Validation consists in confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.

Change control

In case of changes in the software, the validation status needs to be re-established. If a revalidation analysis is needed, it should be conducted not just for validation of the individual

change, but also to determine the extent and impact of that change on the entire computerised system.

In the same way, changes in the computer environment could have an impact on the software running. In this case, a revalidation could be required.

In both cases, the extent of the revalidation will depend on the nature of the change. The nature of the changes should be documented.

Automatic updates should ideally be controlled by IT or a system administrator and installed at pre-defined dates to minimize both disruption and unexpected behaviour of the system. Following installation of updates, verification should be carried out, the extent of which will depend on the extent of the update(s). Each update should be documented.

Note: this does not necessarily apply to service patches for commercial office software.

Verification of the software

Commercial software should be checked at installation.

Concerning in-house software, it should be verified not only at installation but also on a regular basis to avoid any error and guarantee good results. The regularity of the verification depends on software safety, usage frequency and the possible impact, if there is a failure.

In both cases, the OMCL's policy should be described in a procedure.

Protection of the software

Software must be protected against any intrusion that could generate wrong scientific results. One way could be to secure software or computers/systems access by a password. It must also be protected against any external interference that could change the data and affect the final results.

Backup

Traceability must be ensured from raw data to results. If all or part of the traceability of parameters relevant for the quality of the results is available only in electronic form, a backup process must be implemented to allow for recovery of the system following any failure which compromises its integrity. Back up frequency depends on data criticality, amount of stored data and frequency of data generation.

The OMCLs should have a policy and procedure in place for ensuring the integrity of backups (secure storage location, adequately separated from the primary storage location, etc) – this may be part of a more general 'disaster recovery plan'.

A procedure for regular testing of backup data (restore test), to verify the proper integrity and accuracy of data, should be also in place.

Archive of superseded software versions

Superseded versions of software should be archived (if required for access to historical data) for at least 5 years[1] in a retrievable and readable electronic format.

Note: this requirement is not applicable to commercial off-the-shelf office software (including service patches), software that is archived by a qualified subcontractor or when historical data (raw data and results) are documented in paper format

Identification of software version

The version and name of the software should be displayed to the user at an appropriate stage of the operation of the software (e.g. on the screen when opening the application) and it should be traceable in any reports generated by the software.

For laboratory software on computers as part of test equipment, software updates including the version number should be traceable in the equipments' log book.

Review of computerised systems

Risk management activities and/or audits should be performed on a regular basis for computerised systems.

Training of software operators

Correct operation of the software should be ensured. This may be done either by appropriate and documented training or through detailed information in the relevant SOPs.

3. VALIDATION OF CALCULATION SOFTWARE

Commercial or in-house developed software may be used for calculation and data analysis.

The requested documentation/information, applicable to both commercial and for in-house developed software for calculations, is shown in Table I.

a) Commercial software

If several pieces of commercial software are available, the laboratory should select the one that better fits the intended purpose.

According to ISO/IEC 17025 standard[2], commercial off-the-shelf software (e.g. word-processing, database and statistical programmes), in general use within their designed application range, may be considered to be sufficiently validated. However, laboratory software configurations/modifications should be validated.

[1] OMCL Guideline "ARCHIVING WITHIN THE OMCL NETWORK"
[2] ISO/IEC 17025 standard, chapter 5.4.7 and 5.5.5.

A reduced validation procedure (of these configurations/modifications) is acceptable if the documentation supplied with the commercial off-the-shelf product has been reviewed and considered as fulfilling the user requirements.

b) In-house software

If in-house software are used, they are under the supervision of the main user; they must be validated, checked and secured. For more details on validation, see Annex 1.

General requirements:

- Concerning spreadsheets (e.g. Excel®), for security reasons, all cells including calculations must be locked in such a way that formulas are not accidentally overwritten. Free access should only be given to cells to be filled in with data. Formulas should also be protected from accidental input of inappropriate data type (e.g. text in a numeric field).
- Each calculation algorithm should be tested with another validated software (the software version used for the calculations should be traceable in the records) or by a pocket calculator and documented or in comparison with published data.
- A known dataset should be used for the verification of the software, for which the expected final results are identified.

Table I: Software documentation

Information/documentation that should be available	Commercial	In-house
Name, version and unique identification of the software	X	X
Original files (CD-ROM…) or storage location to install the software and software to manage the computer environment	X	X
Date at which the software was put into operation	X	X
Current physical location, where appropriate	X	X
Responsible person in charge of the software	X	X
Manufacturer's name, licence number and serial number or other unique identification	X	
Conditions under which the software runs, where applicable (hardware, operating system,…)	X	X
Manufacturer's certificate of validation, if available	X	
Manufacturer's instructions, if available, or reference to their location	X	
Documentation on validation of configurations/modifications performed by the user that may impact the results (see Annexes)	X	
Name of the person who developed and validated the software, and the date of validation		X
Source code, if available		X
Operating rules, where appropriate		X
Documentation on software regular verification		X
Documentation on software validation (see Annexes)		X
Follow-up of encountered failures, maintenance of the process, updated versions and , where appropriate, configuration management	X	X

4. VALIDATION OF DATABASE COMPUTERISED SYSTEMS

Databases used for the storage and retrieval of test results and preparation of test reports, which have been developed in-house by using commercial software (e.g. Access®), in its normal configuration, are considered to be sufficiently validated.

Nevertheless, the following minimum documentation/information has to be kept up to date, in the corresponding file of each database:

- A schematic representation of the database.
- Changes to forms, queries, macros, field types or properties that could have an impact on the quality of results should be traceable.
- Each user should have a personal access code.
- User rights should be defined.
- Operating rules should be recorded.
- Any modification for improvement or failure should be documented.

5. VALIDATION OF LIMS and ELN

For commercial Laboratory Information Management System (LIMS) and Electronic Laboratory Notebook (ELN), system validation must ensure that the entire system has been properly tested. For more details on validation, see Annex 2.

Validation of any modification, configuration or calculation that may have an impact on the results are under the users' responsibility (see chapter 3.a and table 1 for commercial software).

6. VALIDATION OF COMPUTERS AS PART OF TEST EQUIPMENT

In some test methods (e.g. HPLC, particle counting), test equipment is used, which is controlled by computerised systems. In doing so, the raw data are in general also evaluated directly via the computer. The quality of such test results is thus largely dependent on the correct use of the software and the functionality of the computerised system. For more details on validation, see Annex 3.

As part of the equipment qualification, the computerised system, together with the software relating to it must be validated with regard to reliability, accuracy, and reproducibility (it may however be sufficient to qualify the testing equipment with the software as a whole).

A revalidation is required if modifications to the computerised systems (hardware or software) might influence the quality of the test results.

REFERENCES

For all references, the latest version applies.

1) Good Automated Manufacturing Practices (GAMP).
2) Good Practices for Computerized Systems in regulated "GXP" environments. Pharmaceutical Inspection Convention/Pharmaceutical Inspections Co-operation Scheme (PIC/S).
3) EU Guidelines to Good Manufacturing Practice (GMP). Annex 11. Computerized Systems.
4) OECD Series on Principles of Good Laboratory Practices and Compliance Monitoring. Number 10. The Application of the Principles of GLP to Computerized Systems. Environment Monograph no. 116.
5) U.S. Food and Drug Agency (FDA) General Principles of Software Validation; FDA Glossary of computerized system and software development terminology (http://www.fda.gov/ora/inspect_ref/igs/gloss.html).

LIST OF ANNEXES (the latest version applies):

- Annex 1: Validation of computerised calculation systems - PA/PH/OMCL (08) 87
- Annex 2: Validation of databases, Laboratory Information Management Systems (LIMS) and Electronic Laboratory Notebooks (ELN) - PA/PH/OMCL (08) 88
- Annex 3: Validation of computers as part of test equipment - PA/PH/OMCL (08) 89