Concept Paper on the revision of Annex 11 of the guidelines on EU GMP for medicinal products – Computerised Systems

This concept paper addresses the need to update Annex 11, Computerised Systems, of the Good Manufacturing Practice (GMP) guide. Annex 11 is common to the member states of the European Union (EU)/European Economic Area (EEA) as well as to the participating authorities of the Pharmaceutical Inspection Co-operation Scheme (PIC/S). The current version was issued in 2011 and does not give sufficient guidance within a number of areas. Since then, there has been extensive progress in the use of new technologies.

Reasons for the revision of Annex 11 include, but are not limited to the following (in non-prioritised order and with references to existing sections in sharp brackets). More improvements may prove to be necessary as inputs will be received by the drafting group:

The amendments to the 33 points in the current version are as follows:

1. [New] The document should be updated to replace relevant parts of the Q&A on Annex 11 and the Q&A on Data Integrity on the EMA GMP website.

2. [New] With regards to data integrity, Annex 11 will include requirements for ‘data in motion’ and ‘data at rest’ (backup, archive and disposal). Configuration hardening and integrated controls are expected to support and safeguard data integrity; technical solutions and automation are preferable instead of manual controls.

3. [New] An update of the document with regulatory expectations to ‘digital transformation’ and similar newer concepts will be considered.

4. [Principle] The scope should not only cover where a computerised system “replaces of a manual operation”, but rather, where it replaces ‘another system or a manual process’.

5. [1] References should be made to ICH Q9.

6. [3.1] The list of services should include to ‘operate’ a computerised system, e.g. ‘cloud’ services.

7. [3.1] For critical systems validated and/or operated by service providers (e.g. ‘cloud’ services), expectations should go beyond that “formal agreements must exist”. Regulated users should have access to the complete documentation for validation and safe operation of a system and be able to present this during regulatory inspections, e.g. with the help of the service provider. See also Notice to sponsors and Q&A #9 on the EMA GCP website and Q&A on the EMA GVP website)

8. [3.3] Despite being mentioned in the Glossary, the term "commercial off-the-shelf products" (COTS) is not adequately defined and may easily be understood too broadly. Critical COTS products, even those used by "a broad spectrum of users" should be qualified by the vendor or by the regulated user, and the documentation for this should be available for inspection. The use of the term and the expectation for qualification, validation and safe operation of such (e.g. 'cloud') systems should be clarified.

9. [4.1] The meaning of the term 'validation' (and 'qualification'), needs to be clarified. It should be emphasised that both activities consist of a verification of required and specified functionality as described in user requirements specifications (URS) or similar.

10. [4.1] Following a risk-based approach, system qualification and validation should especially challenge critical parts of systems which are used to make GMP decisions, parts which ensure product quality and data integrity and parts, which have been specifically designed or customised.

11. [4.4] It is not sufficiently clear what is implied by the sentence saying "User requirements should be traceable throughout the life-cycle". A user requirements specification, or similar, describing all the implemented and required GMP critical functionality which has been automated, and which the regulated user is relying on, should be the very basis for any qualification or validation of the system, whether performed by the regulated user or by the vendor. User requirements specifications should be kept updated and aligned with the implemented system throughout the system life-cycle and there should be a documented traceability between user requirements, any underlying functional specifications and test cases.

12. [4.5] It should be acknowledged and addressed that software development today very often follows agile development processes, and criteria for accepting such products and corresponding documentation, which may not consist of traditional documents, should be clarified.

13. [6] Guidelines should be included for classification of critical data and critical systems.

14. [7.1] Systems, networks and infrastructure should protect the integrity of GMP processes and data. Examples should be included of measures, both physical and electronic, required to protect data against both intentional and unintentional loss of data integrity.

15. [7.2] Testing of the ability to restore system data (and if not otherwise easily recreated, the system itself) from backup is critically important, but the required periodic check of this ability, even if no changes have been made to the backup or restore processes, is not regarded necessary. Long-term backup (or archival) to volatile media should be based on a validated procedure (e.g. through

'accelerated testing'). In this case, testing should not focus on whether a backup is still readable, but rather, validating that it will be readable for a given period.

16. [7.2] Important expectations to backup processes are missing, e.g. to what is covered by a backup (e.g. data only or data and application), what types of backups are made (e.g. incremental or complete), how often backups are made (all types), how long backups are retained, which media is used for backups, and where backups are kept (e.g. physical separation).

17. [8] The section should include an expectation to be able to obtain data in electronic format including the complete audit trail. The requirement to be able to print data may be reconsidered.

18. [9] An audit trail functionality which automatically logs all manual interactions on GMP critical systems, where users, data or settings can be manually changed, should be regarded as mandatory; not just 'considered based on a risk assessment'. Controlling processes or capturing, holding or transferring electronic data in such systems without audit trail functionality is not acceptable; any grace period within this area has long expired.

19. [9] The audit trail should positively identify the user who made a change, it should give a full account of what was changed, i.e. both the new and all old values should be clearly visible, it should include the full time and date when the change was made, and for all other changes except where a value is entered in an empty field or where this is completely obvious, the user should be prompted for the reason or rationale for why the change was made.

20. [9] It should not be possible to edit audit trail data or to deactivate the audit trail functionality for normal or privileged users working on the system. If these functionalities are available, they should only be accessible for system administrators who should not be involved in GMP production or in day-to-day work on the system (see 'segregation of duties').

21. [9] The concept and purpose of audit trail review is inadequately described. The process should focus on a review of the integrity of manual changes made on a system, e.g. a verification of the reason for changes and whether changes have been made on unusual dates, hours and by unusual users.

22. [9] Guidelines for acceptable frequency of audit trail review should be provided. For audit trails on critical parameters, e.g. setting of alarms in a BMS systems giving alarms on differential pressure in connection with aseptic filling, audit trail reviews should be part of batch release, following a risk-based approach.

23. [9] Audit trail functionalities should capture data entries with sufficient detail and in true time, in order to give a full and accurate picture of events. If e.g. a system notifies a regulated user of inconsistencies in a data input, by writing an error message, and the user subsequently changes the input, which makes the notification disappear; the full set of events should be captured.

24. [9] It should be addressed that many systems generate a vast amount of alarms and event data and that these are often mixed up with audit trail entries. While alarms and events may require their own logs, acknowledgements and reviews, this should not be confused with an audit trail review of manual system interactions. Hence, as a minimum, it should be possible to be able to sort these.

25. [11] The concept of configuration review should be added. Instead of taking onset in the number of known changes on a system (upgrade history), it should be based on a comparison of hardware and software baselines over time. This should include an account for any differences and an evaluation of the need for re-qualification/validation.

26. [12.1] The current section has only focus on restricting system access to authorised individuals; however, there are other important topics. In line with ISO 27001, a section on IT security should include a focus on system and data confidentiality, integrity and availability.

27. [12.1] The current version says that “Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons”. However, it is necessary to be more specific and to name some of the expected controls, e.g. multi-factor authentication, firewalls, platform management, security patching, virus scanning and intrusion detection/prevention.

28. [12.1] It should be specified that authentication on critical systems should identify the regulated user with a high degree of certainty. Therefore, authentication only by means of a ‘pass card’ might not be sufficient, as it could have been dropped and later found by anyone.

29. [12.1] Two important expectations for allocation of system accesses should be added either here or elsewhere; i.e. ‘segregation of duties’, that day-to-day users of a system do not have admin rights, and the ‘least privilege principle’, that users of a system do not have higher access rights than what is necessary for their job function.

30. [12.3] The current version says that “Creation, change, and cancellation of access authorisations should be recorded”. However, it is necessary to go further than just recording who has access to a system. Systems accesses and roles should be continually managed as people assume and leave positions. System accesses and roles should be subject to recurrent reviews in order to ensure that forgotten and undesired accesses are removed.

31. [17] As previously mentioned (see 7.2), it is not sufficient to re-actively check archived data for accessibility, readability and integrity (it would be too late to find out if these parameters were not maintained). Instead, archival should rely on a validated process. Depending on the storage media used, it might be necessary to validate that the media can be read after a certain period.

32. [New] There is an urgent need for regulatory guidance and expectations to the use of artificial intelligence (AI) and machine learning (ML) models in critical GMP applications as industry is already implementing this technology. The primary focus should be on the relevance, adequacy and integrity of the data used to test these models with, and on the results (metrics) from such testing, rather that on the process of selecting, training and optimising the models.

33. [New] After this concept paper has been drafted and prepared for approval of the EMA GMP/GDP Inspectors Working Group and the PIC/S Sub-committee on GMDP Harmonisation, the FDA has released a draft guidance on Computer Software Assurance for Production and Quality System Software (CSA). This guidance and any implication will be considered with regards to aspects of potential regulatory relevance for GMP Annex 11.

Reference: 重磅，歐盟發佈新版 **EU GMP** 附錄 **11**《電腦化系統》概念文件，明確 **Audit trial** 為強制要求**! (qq.com)**